Electronic Surveillance of United States Lawyers

George M. KRAW

United States authorities eavesdrop on attorney communications in a variety of ways and for a variety of reasons, although there are procedural and legal restrictions on the monitoring. Attorneys can have their phones wiretapped when they become entangled in activities that may further a crime. Conversations can be monitored when an attorney speaks with a party whose phone is tapped. More recently, the growth of surveillance technology has made it possible for law enforcement and intelligence agencies to go beyond eavesdropping on individual conversations and monitor so-called electronic "metadata" – who you are, who you call, how long you talk, what you do on the Internet – that can be more useful to them than message content. Former National Security Agency general counsel Stewart Baker claims that "Metadata absolutely tells you everything you need to know about somebody's life. If you have enough metadata, you don't really need content."

The current standards for monitoring attorney communications – in both national security matters as well as ordinary criminal investigations – are discussed later in this article. These rules usually, but not always, require a judicial order for which law enforcement must submit a full statement of the facts to the judge hearing the surveillance application. The Foreign Intelligence Surveillance Court, also known as the FISA Court, oversees requests for warrants against suspected foreign intelligence agents inside the United States. But the immediate question for United States lawyers goes beyond whether these standards are adequate to shield confidential attorney-client relationships – they are not – to whether they are even relevant to the new technologies. The extent to which surveillance technology has moved past the need to intercept content in order to understand a communication's meaning and import is unclear, but there is plainly a furious effort being undertaken to just that end. Relying upon the NSA to protect constitutional safeguards and civil liberties against the inroads of technology is problematic at best. Like most intelligence agencies worldwide, the NSA prefers to ask forgiveness after the fact rather than permission beforehand, and what mischief it is currently up to may not be fully understood even by its nominal overseers in the United States Congress.

Rules for protecting attorney-client conversations are based upon ancient English common law concepts of attorney-client privilege that chiefly protect the content of conversations. If Stewart Baker is correct, access to such content already is unnecessary to obtain much confidential information that the attorney-client privilege is designed to shield. Of course, it may turn out that Baker's claims were hyperbolic and disproven by subsequent events. For now, the NSA are true believers in the power of metadata. At a recent public debate on privacy rights, General Michael Hayden, a former director of both the Central Intelligence Agency and the NSA, called the Baker comment "absolutely correct" and added "We will kill people based on metadata."

Rules for protecting attorney-client conversations are based upon ancient English common law concepts of attorney-client privilege that chiefly protect the content of conversations.

The rapid development of surveillance capabilities directly affecting confidential relationships, together with other robust actions undertaken in post 9/11 national security initiatives have left many of those American lawyers on the front lines of these issues uncertain and confused about the proper response to aggressive monitoring of both their communication content and activity. The Nation magazine reports that lawyers in national security cases in the prior decade found themselves confronted by law enforcement transcripts of their own confidential conversations with clients, in what some characterized as attempts to intimidate. Defense counsel Lynne Stewart was prosecuted, convicted and sentenced to prison for providing material support to terrorists on the basis of video and audio surveillance recordings of herself and her client Sheik Abdel Rahman. In 2008, Justice Department officials told the New York Times that in the past they had not used their terrorist surveillance powers to single out lawyers but future telephone calls "involving such persons would not be categorically excluded." The Times further reported that several Guantanamo defense lawyers, including partners at large corporate law firms, said that monitoring had made them change the way they went about their work apart from Guantanamo cases. A defense lawyer from Chicago, H. Candace Gorman, said in a 2008 affidavit that she was no longer accepting new clients of any type because she could not assure them of confidentiality. One of the revelations of Edward Snowden was that Australia, a foreign intelligence partner of the United States, had monitored and then shared with the NSA, an American law firm's confidential communications with its client, the Republic of Indonesia, about a trade dispute involving clove cigarettes – a situation as ludicrous as it is troubling.

These revelations led the American Bar Association to confront the NSA directly on the protection of the confidentiality of attorney-client communications. The NSA's response acknowledged the importance of attorney-client confidentiality without committing to additional specific protections. Earlier, in 2012, the ABA had revised its ethics rules to require lawyers to "make reasonable efforts" to protect confidential

information from unauthorized disclosure to outsiders. It has published a brief guide to possible technological solutions to prevent monitoring of electronic communications. Technological solutions are the preferred fix of Silicon Valley, many of whose companies of late have sought to distance themselves from United States government surveillance activities. However, such technological resolutions rely upon the effectiveness and trustworthiness of the hardware devices and software programs, many of which have been found to have "back doors" which allowed them to be compromised by intelligence and other governmental agencies.

Attorney-client conversations are protected communications in the United States

United States legal protections against eavesdropping on attorney-client conversations are rooted in the legal concept of attorney-client privilege for confidential communications. The privilege derives from English common law and is set out in the Federal Rules of Evidence. Eight factors must be satisfied for the common law attorney-client privilege to apply to a communication. The communication must be (1) legal advice sought from a (2) professional legal advisor (3) where the communication is related to the legal purpose, and (4) is made in confidence, (5) by the client, and (6) is permanently protected for the client (7) from disclosure by himself or the legal advisor, (8) unless that protection is waived. The privilege can be waived by the client or when confidential communications are disclosed to third parties. In addition, the crime-fraud exception can moot the privilege if communications between an attorney and client are themselves used to further a crime or fraud.

United States wiretapping laws and attorney communications with clients and non-clients

In Katz v. United States, 389 U.S. 347 (1967), the United States Supreme Court refined prior definitions prohibiting unreasonable searches and seizures under the United States constitution to include electronic surveillance where there is a reasonable expectation of privacy. In Berger v. New York, 388 U.S. 41 (1967) the Court invalidated a state law under the Fourth Amendment, because the statute authorized electronic eavesdropping without required procedural safeguards. These decisions led to the federal wiretap statute, originally passed in 1968 and sometimes called "Title III" or the "Wiretap Act," that generally requires that federal law enforcement obtain a wiretap order before monitoring or recording electronic communications, and does not distinguish attorney conversations. United States law gives more protection against government eavesdropping than it does against physical searches because eavesdropping violates not only the targets' privacy, but also the privacy of everyone with whom they communicate. The Supreme Court has stated that since eavesdropping violates so many individuals' privacy, law enforcement agencies should only be allowed to wiretap when investigating serious crimes. The Wiretap Act contains enumerated crimes that are the only ones that can be investigated with a wiretap order. The Wiretap Act requires law enforcement to obtain a wiretap order whenever they want to "intercept" an "oral communication," an "electronic communication," or a "wire communication." Interception of those communications is commonly called surveillance. These rules apply to both attorney and non-attorney communications.

Spoken communications are protected when an individual has a reasonable expectation that the conversation will not be recorded. If law enforcement wants to install a microphone or a "bug" in a house or office, they must obtain a wiretap order. The government may attempt to use a target's own microphones – for example, by obtaining the phone company's cooperation to turn on a target's cell phone microphone and eavesdrop on nearby conversations. A wire communication is any voice communication that is transmitted over phone company wires, cellular networks or the Internet. There is no need to have a reasonable expectation of privacy for the statute's protections to apply, although radio broadcasts and other communications that can be received by the public are not protected. If the government wants to tap any target's phone calls – landline, cellphone, or Internet-based – it has to obtain a wiretap order. An electronic communication is any transmitted communication that is not a voice communication. This includes all non-voice Internet and cellular phone activities like email, instant messaging, texting and web surfing. It also covers faxes and messages sent with digital pagers. As with wire communications, it is not necessary to have a reasonable expectation of privacy in electronic communications for them to be protected by the statute.

Although the federal government may get a warrant to "intercept" a target's communications, it is not allowed to prevent the communication from occurring. The government cannot stop calls, block emails, or otherwise interfere with communications based on an intercept order. The Wiretap Act makes it a crime for anyone that is not a party to a communication to intercept the communication, unless at least one of the parties has previously consented. These rules apply to lawyers and non-lawyers alike. Many state wiretap laws, including California's, require all parties to consent, but those laws control state and local policy, not federal law agents. If the local area police want to intercept an oral, wire, or electronic communication to which they are not a party and for which they have no consent, they must obtain a wiretap order. An undercover police officer or informant talking to an attorney who is a target while wearing a wire is a party to the conversation and has consented to the interception. Wiretap law also does not protect targets from government eavesdroppers that simply overhear attorney conversations without electronic interception.

Surveillance of attorney-client communications by the NSA

Most attorney-client conversations do not get special protections under United States law from NSA eavesdropping, and the FISA Court itself is a friendly venue for government action. According to government records obtained by the Electronic Privacy Information Center, of the almost 34,000 surveillance requests made to the FISA Court in the last 35 years, only 11 have been rejected.

The Wiretap Act and the Foreign Intelligence Security Act of 1978 created a statutory framework that purported to bring government eavesdropping under the rule of law. The post-9/11 innovations that endanger attorney-client communications have separate roots. Under FISA section 215, Congress expanded the business records collection powers in a way that has resulted in the bulk metadata collection that reveals so much (but is novel on attorney-client privilege since content is not disclosed). Separately, in 2008, Congress passed the FISA Amendments Act, which the Snowden disclosures revealed scoop up content of Americans, including lawyers, communicating overseas electronically. As a consequence law

firms and other groups increased encryption services and – in true spy versus spy fashion – the government now can use encryption as a reason for longer storage and viewing communications with suspicion, while seeking improved surveillance alternatives from metadata.

In Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013), the Supreme Court rejected a challenge to a 2008 law allowing warrantless wiretapping that was brought in part by lawyers with foreign clients, who were likely targets of NSA monitoring. The lawyers contended that the law raised risks that required them to take costly measures, like traveling overseas to meet clients, to protect sensitive communications. The Supreme Court dismissed their fears as "speculative." The NSA is prohibited from targeting Americans, including businesses, law firms and other organizations based in the United States, for surveillance without warrants. Intelligence officers have repeatedly said that the NSA does not use the spy services of its partners in the so-called Five Eyes alliance – Australia, Britain, Canada and New Zealand – to avoid U.S. law. However, the NSA can intercept the communications of Americans, including lawyers, if they are in contact with a foreign intelligence target abroad, such as what occurred with the Indonesian officials monitored in the clove cigarette dispute. In such situations, the NSA is required to follow up to protect the U.S. citizens' privacy – so-called "minimization procedures' – by taking actions such as deleting the identities of the Americans or deleting information that is not deemed necessary to assess the foreign intelligence before further sharing this information with other government agencies. The minimization procedures are regulations issued pursuant to the Foreign Intelligence Surveillance Act. These regulations dictate when NSA agents can monitor communications. Section four of the previously classified 2011 guidelines, states that an agent also must cease monitoring after determining that he or she is monitoring an attorney-client communication of an individual who has been charged under United States law.

The USA Freedom Act

The USA Freedom Act, pending in Congress as of June, 2014, is designed to restrict the mass collection of data by the NSA. It has both bipartisan support and bipartisan opposition, with attitudes toward the bill not dividing evenly along Republican and Democrat party lines. As originally drafted, the legislation was supposed to end the bulk collection of Americans' metadata, end certain secret laws created by the Foreign Intelligence Surveillance Court, and introduce a "Special Advocate" to represent public privacy matters. The Special Advocate could presumably address issues of monitoring confidential attorney-client relationships and communications as they arose. Other proposed changes include limits to government programs like PRISM, which incidentally retains U.S. individuals' Internet data, and providing greater transparency by allowing companies such as Google and Facebook to disclose information about government demands for information. The initial legislative draft has been significantly amended. Although the current version does not provide specific protection for attorneys, the legislation may eventually provide some additional protections for attorney communications by restricting the ability of the NSA to monitor electronic communications.

The evolving rules for surveillance of lawyer communications in an age of rapidly advancing technological capabilities have become enmeshed in the broader American debate about balancing individual privacy and civil liberties versus protecting civil society against security threats. The confidentiality of attorney-client communications is a fundamental concept of United States jurisprudence and central to trust in the operation of the justice system. Such traditional legal protections may be diminished or vitiated through the use of new tools by government and private agencies. The challenge now is to prevent such changes to the law from occurring by default, thereby bypassing the democratic and judicial processes.

George M. KRAW
Kraw Law Group
Mountain View, CA, United States
gkraw@kraw.com

Sources for this article and for further reading:

Stewart Baker's quote is from "Can the NSA Be Controlled" by David Cole in The New York Review of Books, June 19, 2014. The statement by General Michael Hayden is also from this article, which is part of a series that Professor Cole has written for the NYR about civil liberties and national security. This article also contains a discussion of the USA Freedom Act.

Article V, Rules 501 and 502 of the Federal Rules of Evidence address attorney-client privilege.

The New York Times has extensive coverage of surveillance matters on its web archive. NY Times Reporter Benjamin Weiser has a summary of the Lynne Stewart case in "10-Year Sentence for Lawyer in Terrorism Case Is Upheld" June 28, 2012 **www.nytimes.com/2012/06/29/nyregion/lynne-stewarts-10-year-prison-sentence-is-upheld.html?_r=0.**

NSA spying on United States lawyers was reported by James Risen and Laura Poitras in "Spying by NSA Entangled U.S. Law Firm, New York Times, February 15, 2014 **www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=0.** See also Nicholas Niarchos "Has the NSA Wiretapping Violated Attorney-Client Privilege?" The Nation, February 4, 2013 **www.thenation.com/article/178225/has-nsa-wiretapping-violated-attorney-client-privilege**

The NSA's assurances concerning lawyer-client confidentiality are contained in a letter to the American Bar Association; the correspondence can be found online at **www.americanbar.org/content/dam/aba/images/abanews/nsa_response_031020l4.pdf.**

The Director of National Intelligence maintains a blog **icontherecord.tumblr.com** to address current issues.

The New York Times **www.nytimes.com**, the Guardian **www.theguardian.com** and Der Spiegel **www.derspiegel.de** websites all have extensive coverage of the Snowden matter.

The previously classified 2011 NSA minimization procedures can be found online at **www.aclu.org/files/assets/minimization_procedures_used_by_nsa_in_connection_with_fisa_sect_702.pdf**

The Wiretap Act is part of Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510-2522 (2002). The Electronic Freedom Foundation has a useful summary of wiretap rules and privacy rights generally on its website eff.org at **https://ssd.eff.org/wire/govt/wiretapping-protections**