SYRACUSE UNIVERSITY

COLLEGE OF LAW
Professor Nathan A. Sales
Dineen Hall
950 Irving Avenue
Syracuse, New York 13244-6070
315.443.3121
nasales@law.syr.edu

July 15, 2015

I understand that the Conseil Constitutionnel is currently reviewing a new law that would expand France's authority to conduct surveillance of suspected terrorists. L'Ordre des avocats de Paris has asked me to prepare a short analysis comparing this legislation to the surveillance laws in the United States, especially the laws that regulate government monitoring of privileged attorney-client communications. I hope that the following observations will be helpful as France considers how to address these important issues. In short, the new legislation broadly authorizes warrantless surveillance and appears to lack any limits on the monitoring of privileged communications between attorneys and their clients. This stands in contrast to U.S. law, which generally requires a court order for domestic surveillance and which imposes several basic restraints on the government's ability to collect, disseminate, and use certain communications that are protected by the attorney-client privilege. Policymakers in France might wish to consider comparable safeguards to ensure that necessary surveillance of dangerous terrorists does not unduly interfere with fundamental rights and freedoms.

By way of background, I am Associate Professor of Law at Syracuse University College of Law, where I teach and write in the fields of national security law and counterterrorism law. Before entering academia I held a number of national security positions with the United States government. For instance, I was Deputy Assistant Secretary in the Office of Policy at the U.S. Department of Homeland Security, where my work focused on intelligence gathering, information sharing, and terrorist travel. Prior to that, I was Senior Counsel in the Office of Legal Policy at the U.S. Department of Justice, where I helped write and implement the USA PATRIOT Act, the Attorney General's investigative guidelines, and other counterterrorism initiatives. These experiences have helped inform my thinking on the important question of how to balance the government's national-security needs against the equally important need to preserve privacy, civil liberties, and other basic values.

The Fourth Amendment to the United States Constitution generally requires government officials to obtain a court order before intercepting a suspect's communications. This warrant requirement applies to routine criminal cases, *Katz v. United States*, 389 U.S. 347 (1967), as well as domestic national security investigations, *United States v. U.S. District Court*, 407 U.S. 297 (1972). The latter are regulated by a statute known as the Foreign Intelligence Surveillance Act of 1978 (FISA). FISA provides that the government ordinarily may not conduct electronic surveillance unless it first convinces a federal judge that there is probable cause to believe that

the target is an "agent of a foreign power"—i.e., a spy or terrorist. 50 U.S.C. § 1805(a)(2). The U.S. Supreme Court has explained that prior judicial approval serves as an important check on overzealous surveillance. Interposing a "neutral and detached magistrate[]" between government officials and citizens "accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government." *U.S. District Court*, 407 U.S. at 317. The warrant requirement thus helps protect a number of basic rights and liberties, including privacy and the freedom of speech. *Id.* at 313-14.

In 2008, Congress enacted a limited exception to FISA's warrant requirement. Under section 702 of FISA, the government may—without a court order—monitor non-Americans who are "reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). It is important to note that section 702 only permits warrantless surveillance of *non-citizens* who are *outside* the United States. If the government wishes to monitor Americans anywhere in the world, or non-citizens inside the country, it must first obtain a warrant from a federal court pursuant to traditional FISA standards and procedures. *Id.* § 1881a(b)(1)-(3). Unlike section 702, which is a limited exception to the default rule in the United States that electronic surveillance normally requires a court order, France's new law appears to broadly authorize warrantless monitoring in a wide range of circumstances.

U.S. law also has long regarded the attorney-client privilege as a fundamental element of the legal system. According to the Supreme Court, "[t]he attorney-client privilege is the oldest of the privileges for confidential communications known to the common law." *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). The purpose of the privilege is to "encourage full and frank communication between attorneys and their clients," *id.*, which would not be possible if government officials or other outsiders were listening in. The privilege "thereby promote[s] broader public interests in the observance of law and administration of justice." *Id*.

At the same time, there is a risk that criminals might abuse the attorney-client privilege by enlisting their lawyers in their unlawful schemes. In 2000, Omar Abdel Rahman—a cleric who was convicted of masterminding the 1993 World Trade Center bombing and a number of other terrorist plots—used his lawyer to smuggle messages out of jail to extremists in Egypt urging them to repudiate a ceasefire agreement and resume a campaign of violence. *United States v. Stewart*, 686 F.3d 156, 161-63 (2d Cir. 2012). This is why U.S. law has long recognized a "crime-fraud" exception to the attorney-client privilege, under which the privilege does not extend to communications "made in furtherance of a future crime or fraud." *United States v. Zolin*, 491 U.S. 554, 563 (1989).

U.S. law attempts to strike an appropriate balance between preserving attorney-client confidentiality and preventing abuse of the privilege, and it limits the government's ability to monitor certain communications between attorneys and their clients in national security investigations.

For example, FISA expressly provides that "[n]o otherwise privileged communication obtained in

accordance with, or in violation of, [FISA] shall lose its privileged character." 50 U.S.C. § 1806(a). According to the leading treatise on U.S. national security law, this statute ensures that "a conversation between a FISA target and his attorney that is otherwise subject to the attorney-client privilege remains privileged even though federal agents are monitoring the conversation on a FISA wiretap." 2 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS § 28.6, at 221 (2d ed. 2012).

Section 702 of FISA further seeks to protect the privilege through so-called "minimization" procedures. 50 U.S.C. § 1881a(e) (requiring the Attorney General to adopt minimization procedures and directing a federal court to review the procedures); *see also id*. § 1801(h) (requiring minimization procedures for traditional FISA surveillance). When the government conducts surveillance, it is inevitable that it will collect a large amount data that is unrelated to the investigation. U.S. law addresses this problem with rules that restrict which personnel may see information that has been collected inadvertently, the purposes for which the information may and may not be used, how long it may be retained, and so on. *See generally Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (Oct. 31, 2011), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

The section 702 minimization procedures generally oblige the government to destroy any non-pertinent data about an American that has been incidentally acquired during surveillance—a requirement that applies to privileged information as well as non-privileged information. *Id*. § 3(b)(1). The rules also bar the government from disseminating any information about an American—privileged or non-privileged—unless it indicates that he is engaging in terrorism, is evidence of a crime, or similar criteria are met. *Id.* § 6(b).

In addition to these general rules, there are special requirements for privileged attorney-client communications:

> As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed disseminations of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination.

Id. § 4.

These minimization requirements—like section 702 in general—only apply to the surveillance of non-Americans who are outside the United States. The minimization procedures for traditional FISA surveillance remain classified, so there is no definite, publicly-available guidance on what steps the government takes to protect attorney-client communications in that context. While this is only speculation, it seems unlikely that the protections under traditional FISA (which governs surveillance of Americans) would be *weaker* than those under section 702 (which governs surveillance of non-Americans).

The legislation under review by the Conseil Constitutionnel appears to lack comparable safeguards for privacy, freedom of speech, and the attorney-client privilege. In light of the terrorist threat that France faces—a threat vividly illustrated by the *Charlie Hebdo* attacks—it is essential that counterterrorism investigators have the legal tools they need to monitor extremists to prevent future atrocities. It is possible to conduct this necessary surveillance in a way that preserves basic rights and liberties. Yet the new law establishes warrantless monitoring as the default form of surveillance (rather than, as in the United States, an exception to the normal requirement of prior judicial approval). Because there is no opportunity for independent and neutral judges to decide whether surveillance of a particular target is justified, there is a heightened risk that government officials might engage in improper monitoring. In addition, the new law does not require the government to adopt minimization procedures or take other steps to reduce the burdens that surveillance can place on attorney-client communications and other confidential information.

Thank you for the opportunity to address this important issue. I hope that this description of U.S. surveillance laws and practices will help inform France's deliberations over how to improve its counterterrorism capabilities while maintaining its fundamental legal values.

Respectfully submitted,

Nathan A. Sales
Associate Professor of Law
Syracuse University College of Law