Transnational Wiretaps and the Fourth Amendment

by KRISTOPHER A. NELSON*

Introduction

A fundamental point of contention in a democratic society is finding the balance between the need for security and the desire for liberty. In the United States, the Fourth Amendment to our constitution is the cornerstone of this balancing act:

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.¹

Since 1789, as the interests of society have shifted, the courts’ interpretation and application of this language has changed as well. Thus, we have moved away from a firm conception of the Fourth Amendment as protecting property interests² to a view based on protecting people from invasions of privacy.³ Nowhere has this shift been more obviously on display than in the treatment of “wiretaps” and other forms of electronic interception of individual’s private communications.

* J.D. Candidate 2009, University of California, Hastings College of the Law; B.A. 1998, University of Washington. I would like to thank James X. Dempsey of the Center for Democracy & Technology for assistance with my early research, and my wife for supporting me throughout the project.

¹ U.S. CONST. amend. IV.


Traditionally, "wiretapping" referred to the interception of communication carried over wires. It began in the 1800s with the widespread adoption of the telegraph and then carried over in the late 1800s and 1900s to the telephone.\(^4\) Originally, "wiretapping" connoted a physical device—the "tap"—which was placed somewhere along the wired connection between the two parties and allowed a third party to intercept the communication.\(^5\) Today, wiretaps may be more virtual than physical, allowing for the interception of, for example, faxes, e-mails, Web traffic and Voice-over-IP communications.\(^6\)

One of the key benefits to wiretaps, especially in modern times, is the anonymity and security provided to the eavesdropper: there is generally no way for the participants in the tapped communication to know if they are being listened to or who is doing the listening. Technically, it is also relatively easy to put a tap in place in the majority of cases. Coupled with the prevalence of people today communicating highly sensitive information over electronic devices, the use of wiretaps is an extremely valuable tool for law enforcement, especially when pursuing organized crime and terrorist groups.

Yet, this same boon to law enforcement presents a strong threat to personal privacy and individual liberty because it is equally possible for governments to abuse this power at the expense of the privacy and individual liberty of its citizens. The Fourth Amendment protects Americans within the borders of the United States, but its applicability outside American territory is less clear.\(^7\) I maintain that Fourth Amendment protections should cover wiretap evidence seized abroad, not just evidence gathered within the United States. These protections should apply whenever a prosecutor seeks to admit such evidence in criminal prosecutions in the United States. Such protections are fundamental whenever the government acts to gather or use evidence—whether that


\(^5\) *Id.*

\(^6\) *Id.*

\(^7\) See, e.g., United States v. Maher, 645 F.2d 780, 782 (9th Cir. 1981) ("Neither our Fourth Amendment nor the judicially created exclusionary rule applies to acts of foreign officials.") (citing United States v. Rose, 570 F.2d 1358, 1361 (9th Cir. 1978); Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1968), cert. denied, 395 U.S. 960 (1969)); Reid v. Covert, 354 U.S. 1, 5-6 (1957) ("The United States is entirely a creature of the Constitution. Its power and authority have no other source. It can only act in accordance with all the limitations imposed by the Constitution. When the Government reaches out to punish a citizen who is abroad, the shield which the Bill of Rights and other parts of the Constitution provide to protect his life and liberty should not be stripped away just because he happens to be in another land."); see also United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976).
evidence was obtained outside the territorial jurisdiction of the United States or not.

However, the practical application of these protections for evidence gathered abroad presents problems. For example, can the United States exercise any control over the methods used to gather evidence by foreign police agencies? Does the exclusionary rule, meant to inculcate a respect for the Fourth Amendment in domestic officials, have any positive role to play in impacting the behavior of non-U.S. agents? Should we judge admissibility based on other countries' laws or should we insist our laws should apply abroad as well? Does it matter if the United States initiated the wiretap or if the foreign country provided the information without direction from the United States? All of these are potentially difficult questions in the context of evidence gathered abroad for use in American criminal courts.

To focus on this problem of wiretap evidence gathered outside the United States, and how this evidence can be admitted into evidence in criminal proceedings, I will look at the United States Constitution and federal case law. Because I am focused on the issue of admitting wiretap evidence into criminal prosecutions, this Note will not examine issues of so-called "warrantless wiretaps" or wiretaps conducted by American intelligence officials abroad for the purposes of intelligence gathering and not criminal prosecutions. However, to the extent that information gathered in such a fashion is admissible in United States criminal courts under current law, this paper will briefly look at the issue of potentially warrantless wiretaps by foreign governments, undirected by the United States.

I. Brief History of Wiretaps in the United States

Finding the proper balance among privacy, security, and law enforcement interests in the realm of wiretapping has always been a complex endeavor. With rapid changes in communications technology quickly reshaping the way people interact, the nation must frequently re-examine its laws to ensure equilibrium among these competing concerns. 8

The foundation of this examination is the Fourth Amendment of the United States Constitution. But it has not always been a stable foundation. Instead, it has shifted over the years as technology and society have changed. For wiretapping, this shift began with the invention of the telegraph in 1844. 9

The first Supreme Court decision involving wiretapping came in 1928, when the Court held, based on the Fourth Amendment language of "persons, houses, papers, and effects," that the Fourth Amendment did not apply to wiretaps unless there was physical trespass by government agents. Six years later, Congress responded with section 605 of the Federal Communications Act of 1934, which provided that "no person not being authorized by the sender shall intercept any communication and divulge or publish [anything about the communication]". The law did not make wiretapping illegal, but rather governed the disclosure of information gathered from wiretaps. The result was that "law enforcement agencies and the government continued to wiretap with increasing frequency."

In the 1960s, public awareness of wiretapping grew, along with a greater realization of how easy wiretapping was to accomplish, and how readily it was capable of being abused. Berger v. New York, decided by the Court in 1967, "addressed for the first time how Fourth Amendment principles apply to a [New York State] court-issued search warrant authorizing the surreptitious interception of communications ...." A five-to-four majority held that New York's law, despite being judicially supervised, violated the Fourth Amendment, and gave seven "constitutional pre-requisites to court-approved monitoring of conversations." In the same year, the Court ruled again that electronic eavesdropping was subject to Fourth Amendment restriction, holding in Katz v. United States that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment ...." Wiretaps, according to the Court, were included in this despite the lack of clear physical intrusion, because the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in

10. U.S. CONST. amend. IV.
14. Id. at 5.
an area accessible to the public, may be constitutionally protected. The twin decisions of *Berger* and *Katz* "made it clear that henceforth the Fourth Amendment, including the warrant requirement and the exclusionary rule, apply to surreptitious surveillance of communications." 19

Congress codified the holdings of *Berger* and *Katz* into federal statute in 1968 as part of Title III. 20 Title III reads in part:

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. 21

In its most basic form, Title III outlawed wiretapping 22 except when law enforcement agents obtained a specific court order. 23 In addition, it limited wiretaps to specific serious crimes and only as a last resort when other investigative techniques had been exhausted. 24 It required that interception of non-relevant communications be minimized. 25 Finally, law enforcement officers were required to notify the target within a specific time period in

---

18. *Id.* at 351–52 (citations omitted).

19. FISHMAN & MCKENNA, *supra* note 12, § 1:4. According to the United States Supreme Court, searches conducted without a warrant are presumptively unreasonable and therefore generally violate the Fourth Amendment. See *Katz*, 389 U.S. at 357; see also FISHMAN & MCKENNA, *supra* note 12, § 1:2(c). The exclusionary rule essentially says that evidence obtained in violation of a defendant's Fourth Amendment rights cannot be used at trial to establish a defendant's guilt. See *Weeks v. United States*, 232 U.S. 383 (1914); see also FISHMAN & MCKENNA, *supra* note 12, § 1:2(b).


22. Note that in 1986, Congress extended Title III when it passed the "Electronic Communications Privacy Act" (ECPA) to apply similar limitations to new electronic communications, including video, text, audio, and other forms of data transmission. Law enforcement agents were now required to obtain a warrant to, for example, intercept and read e-mail. Other forms of internet-based communications were not explicitly included (although ECPA clearly implied they should be) until the passage of the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (USA PATRIOT Act) in 2001. See Wendy Hart & Diana Johnson, *Carnivore: Taking a Bite out of Internet Privacy*, http://gsulaw.gsu.edu/lawand/papers/su03/hart_johnson/.

23. See Boucher et al., *supra* note 13, at 5.

24. *Id*.

25. *Id*. 
order to allow for challenges to probable cause and the conduct of the wiretap. 26

A. Named and Unnamed Parties

"[A] wiretap application must name an individual if the Government has probable cause to believe that the individual is engaged in the criminal activity under investigation . . . ."27 The government may seek a wiretap authorization in order to discover the identities of suspected co-conspirators, and a conversation involving a party not named in the authorization that reveals that party's involvement in the criminal activity under investigation is admissible. 28 Do these unintended third parties have a privacy right that is infringed upon when their conversations are recorded?

The initial warrant is enough to cover all parties whose conversations are intercepted, provided the warrant meets the requirements of Title III. 29 The Supreme Court wrote in United States v. Donovan, "In the wiretap context, [Fourth Amendment] requirements are satisfied by identification of the telephone line to be tapped and the particular conversations to be seized. It is not a constitutional requirement that all those likely to be overheard engaging in incriminating conversations be named." 30 Meeting these requirements thus provides sufficient justification for capturing other, unnamed persons. The Supreme Court, looking at statutory language and legislative history, wrote the following in Kahn:

18 U. S. C. §§ 2518 (1)(b)(iv) and 2518 (4)(a) require identification of the person committing the offense only 'if known' [sic]. The clear implication of this language is that when there is probable cause to believe that a particular telephone is being used to commit an offense but no particular person is identifiable, a wire interception order may, nevertheless, properly issue under the statute. It necessarily follows that Congress could not have intended that the authority to intercept must be limited to those conversations between a party named in the order and others, since at least in some cases, the order might not name any specific party at all. 31

26. Id.
The Court also noted that "the Senate rejected an amendment to Title III that would have provided that only the conversations of those specifically named in the wiretap order could be admitted into evidence."\(^{32}\)

Unintended parties can be "aggrieved person[s]" under Title III.\(^{33}\) Thus, they can contest admissibility of their conversations into evidence.\(^{34}\) In addition, Title III allows "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" to have standing to file a civil suit.\(^{35}\) However, if a third party has their communications intercepted, they only have standing to file a motion to suppress the wiretap evidence if it is to be used against them: "No rights of the victim of an illegal search are at stake," said the Supreme Court, "when the evidence is offered against some other party. The victim can and very probably will object for himself when and if it becomes important for him to do so."\(^{36}\) Noting the enforcement provisions of Title III, the Court went on to say, "[W]e do not deprecate Fourth Amendment rights. The security of persons and property remains a fundamental value which law enforcement officers must respect. Nor should those who flout the rules escape unscathed."\(^{37}\)

B. Wiretap Evidence in Court

Admission of wiretap evidence in United States criminal proceedings is governed by Rules 401 and 402 of the Federal Rules of Evidence which indicate that all "relevant" evidence—that is, evidence "having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable that it would be without the evidence"\(^{38}\)—is admissible, "except as provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority."\(^{39}\) In most court proceedings, although the Fourth Amendment

\(^{32}\) Id. at 157 n.18.

\(^{33}\) See 18 U.S.C. § 2510(11) (2006) ("[A]ggrieved person' means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.").

\(^{34}\) See id. § 2518(10)(a) ("Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter.").

\(^{35}\) See id. § 2520.


\(^{37}\) Id. at 175.

\(^{38}\) FED. R. EVID. 401.

\(^{39}\) Id. at 402 (entitled "Relevant Evidence Generally Admissible; Irrelevant Evidence Inadmissible").
always remains a backdrop, Title III and related statutes are the primary analytic source for determining the admissibility of wiretap evidence.\textsuperscript{40}

To enforce Fourth Amendment protections, the Supreme Court established the "exclusionary rule," designed both to protect criminal defendants from illegally seized evidence as well as to encourage the respect of the Fourth Amendment by officers and agents of the United States.\textsuperscript{41} The Court later extended the exclusionary rule to cover state actors as well, even when the prosecutions occurred in state courts.\textsuperscript{42} The courts have not, however, extended the exclusionary rule to the evidence seized by foreign officials, primarily because the courts have believed that "there is nothing our courts can do that will require foreign officers to abide by our Constitution."\textsuperscript{43}

A core underpinning of Title III was Congress's assumption "that capture of electronic communications would not be an unreasonable intrusion if there were stringent ex parte judicial review before the fact, minimization during a search, and equally stringent adversarial review after the investigation had been completed."\textsuperscript{44} This limited framework supporting restricted wiretaps slowly degraded over the years after the passage of Title III as law enforcement pushed the boundaries of what was permitted and courts and legislatures began to allow them greater latitude in granting warrants.\textsuperscript{45} Nevertheless, Title III gives individuals a framework to contest, via the judicial process, potentially unconstitutional interception of their private communications. Under Title III, individuals have clear statutorily-provided standing to challenge the validity of an intercept, based on factors such as a lack of probable cause, a lack of appropriate safeguards to minimize the intrusion, and so on.\textsuperscript{46}

\begin{itemize}
\item \textsuperscript{41} See Weeks v. United States, 232 U.S. 383 (1914).
\item \textsuperscript{42} See Mapp v. Ohio, 367 U.S. 643 (1961).
\item \textsuperscript{43} Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1968).
\item \textsuperscript{44} James X. Dempsey, \textit{Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy}, 8 ALB. L.J. SCI. & TECH. 65, 85 (1997).
\item \textsuperscript{45} This is evident in six main areas, according to Dempsey: (1) the list of crimes for which wiretapping is allowed has grown from twenty-six in 1968 to ninety-five in 1996; (2) judges rarely deny wiretaps (from 1991 to 2001, judges have only rejected three state or federal wiretap requests, according to the ACLU); (3) the duration of wiretaps has grown as have the number of calls intercepted; (4) the courts now allow wiretapping even when all other techniques have not been exhausted; (5) the "minimization" requirement has not been strictly enforced by the judiciary; and (6) suppression motions are rarely granted (only 4.3 percent of requests were granted between 1985 and 1994). \textit{Id.} at 75–77.
\item \textsuperscript{46} 18 U.S.C. § 2510 (2006).
\end{itemize}
Complicating matters is that, to a greater extent than ever before, the United States is pursuing interceptions of communications in other countries.\textsuperscript{47} This is part and parcel of efforts to fight terrorism and organized crime, amongst other international concerns.\textsuperscript{48} Intentionally or not, these interceptions could involve American citizens or residents, either inside or outside of the United States. Within the borders of the United States, Title III allows judicial oversight and gives standing to impacted individuals to challenge a wiretap, and the Fourth Amendment allows such challenged evidence to be excluded if it does not comport with constitutional standards. But, what happens when the intercept takes place outside the United States?

II. Wiretap Laws Outside the United States

The United States is increasingly collaborating with countries around the world to prosecute crime. Doing so involves significant legal issues which may be easier to understand with a greater background in the laws of other countries with which the United States may cooperate.

A. Canada

The fundamental approach used in Canada to evaluate searches and seizures is remarkably similar to that used in the United States. Part VI of the Criminal Code (entitled “Invasion of Privacy”) is the Canadian counterpart to Title III and deals with the interception of communications, including wiretaps.\textsuperscript{49} Section 8 of the Charter of Rights and Freedoms (the “Charter”) is the Canadian equivalent of the Fourth Amendment and simply reads, “Everyone has the right to be secure against unreasonable

\textsuperscript{47} For example, one report notes,

What the agency calls a “special collection program” began soon after the Sept. 11 attacks, as it looked for new tools to attack terrorism. The program accelerated in early 2002 after the Central Intelligence Agency started capturing top Qaeda [sic] operatives overseas . . . . In addition to eavesdropping on those numbers and reading e-mail messages to and from the Qaeda [sic] figures, the N.S.A. began monitoring others linked to them, creating an expanding chain.


search or seizure."^{50} Cases by the Supreme Court of Canada interpreting Part VI in light of the Charter have resulted in a number of modifications to Canadian law, with a number of amendments passed in 1993 in particular.^{51} As in the United States,^{52} the foundational requirement of Section 8 is "reasonableness,"^{53} and the Supreme Court of Canada has held that for a search to be reasonable it must be (1) authorized by law, (2) the law itself must be reasonable, and, finally, (3) the way in which the search is performed must also be reasonable.^{54}

Specifically looking at wiretaps in *Regina v. Duarte*, the Supreme Court of Canada held that, due to the protections required by the Charter, government monitoring and recording required judicial authorization, even if one of the parties consented to the monitoring.^{55} And as with the Fourth Amendment in the United States, the Supreme Court of Canada has held that Section 8 "protects people and not places."^{56} More recent developments have put into question Canada's emergency wiretap laws, which allow for wiretaps in "exceptional circumstances" without court authorization. In *Regina v. Six Accused Persons*, a judge in British Columbia ruled that section 184.4 of Canada's Criminal Code "is constitutionally invalid legislation" and contravenes "the fundamental freedom to be free from unreasonable search and seizure guaranteed by [Section] 8 of the Charter."^{57}

B. United Kingdom

The Regulation of Investigatory Powers Act 2000^{58} ("RIPA") is the primary legislation that monitors and regulates the lawful interception of

---


52. R. v. Edwards, [1996] 1 S.C.R. 128 (Can.) (analogizing Section 8 protections to rulings by the U.S. Supreme Court regarding search and seizure).

53. Hunter v. Southam Inc., [1984] 2 S.C.R. 145 (Can.) (holding that an assessment of the constitutionality of a search and seizure, or of a statute authorizing a search or seizure, must focus on its "reasonable" or "unreasonable" impact on the subject of the search or the seizure, and not simply on its rationality in furthering some valid government objective).


communications in the United Kingdom. It permits the Secretary of State to issue warrants authorizing the interception of postal services or a public telecommunications system in case of any threat to national security or for preventing or detecting criminal activities. The requirements are not dissimilar to Title III, and make allowances for some amount of judicial oversight and citizen redress for violations. Thus, although warrants are issued by an executive officer, a senior judge reviews the orders and publishes an annual report. In addition, an Investigatory Powers Tribunal considers citizen complaints and can order remedies. Of particular importance is the fact that wiretap evidence, however it is gathered, is currently not admissible in United Kingdom courts. Wiretap material gathered outside of the United Kingdom in accordance with foreign law may be admitted as evidence, however.

Unlike Canada or the United States, the United Kingdom traditionally has had no constitution capable of serving as a basis for rejecting laws passed by its parliament, and thus no equivalent to the protections guaranteed by the Fourth Amendment. Despite this, however, English common law has a long tradition of protecting the same fundamental right embodied in the Fourth Amendment, and the United Kingdom’s membership in the Council of Europe and the European Union means that United Kingdom law is now subject to the European Convention on Human Rights, specifically Article 8 (the right to respect of one’s private and family life).

60. Id.
63. Id. at 9.
64. Id.
65. Id. at 9.
C. Denmark

Like the United Kingdom, Denmark is a member of the Council of Europe and a signatory of the Convention for the Protection of Human Rights and Fundamental Freedoms, more commonly known as the European Convention on Human Rights.68 Thus, it is subject to Article 8 of the Convention, the right to respect of one’s private and family life, the closest analog to the Fourth Amendment.69 As of 1995, Section 191 of the Danish Criminal Code and sections 780 to 791 of the Danish Administration of Justice Act (“Justice Act”) govern searches in Denmark.70 Specifically, Justice Act § 781(1) governs wiretapping, and requires, among other enumerated requirements, “weighty reasons” before a judicial official may authorize a wiretap.71 In addition, Justice Act § 783 outlines procedures for acquiring a wiretap, section 784 provides for an attorney to be appointed for the party being monitored, and section 788 requires notification unless such notification is modified by the supervising court.72 At least one judge has argued that the Danish “weighty reasons” standard is a much lower standard than the Fourth Amendment requires.73

D. The Philippines

The 1987 Constitution of the Republic of the Philippines provides the foundation for analyzing wiretaps in the Philippines. Article III (the “Bill of Rights”), section 2, of the Philippine Constitution is textually identical to the Fourth Amendment to the United States Constitution.74 In addition, section 3 provides additional privacy protections and is as follows:

(1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law. (2) Any evidence

---

70. United States v. Barona, 56 F.3d 1087, 1094 (9th Cir. 1995).
71. Id.
72. Id. at 1095.
73. Id. at 1101 n.7 (Reinhardt, J., dissenting) (“Although we have no way of giving content to what is a meaningless phrase in our own legal system, it is clear from the facts of this case that the Danish standard falls far short of our own probable cause requirement.”).
obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.\textsuperscript{75}

Republic Act 4200 provides the statutory scheme for wiretaps.\textsuperscript{76} It generally requires judicial authorization and limits the crimes for which wiretap orders may be sought.\textsuperscript{77} In general, "Philippine courts have a long history of construing their constitution in favor of individual liberties."\textsuperscript{78} As a result, the Ninth Circuit held in \textit{United States v. Peterson} that a wiretap obtained in the Philippines without judicial authorization violated that country's laws, as it would have in the United States.\textsuperscript{79} In the Republic Act 4200, a public safety exemption does exist, although its scope is unclear.\textsuperscript{80} Expanding on this, the Human Security Act, an anti-terrorism bill, was recently approved.\textsuperscript{81} It provides authorities with much greater power to intercept communications in terrorism-related investigations.\textsuperscript{82} As a result, it is possible that much lower standards might apply to an intercept in some situations in the Philippines than would apply in the United States, especially regarding terrorism, and perhaps especially if the information was to be used outside the Philippines. In addition, "illegal wiretapping continues to remain a problem," and there has been an increase in cases involving wiretapping in the Philippines.\textsuperscript{83}

E. Russia

The Constitution of the Russian Federation recognizes the right of privacy and the security of communications. Article 23 states the following:

Everyone shall have the right to privacy, to personal and family secrets, and to protection of one's honor and good name . . . Everyone shall have the right to privacy of correspondence, telephone communications, mail, cables and other communications.


\textsuperscript{76} An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for other Purposes, Rep. Act No. 4200, (June 19, 1965) (Phil.); see also \textit{Unites States v. Peterson}, 812 F.2d 486, 491 (9th Cir. 1987).

\textsuperscript{77} \textit{Peterson}, 812 F.2d at 491.

\textsuperscript{78} \textit{Id.} (citing Marcelo v. De Guzman, G.R. No. L-29077, 114 SCRA 657 (June 29, 1982). (Phil.))

\textsuperscript{79} \textit{Id.} at 491 ("We decide the case on the assumption that the search did not comply with Philippine law and was, as a result, not reasonable under the fourth amendment.").

\textsuperscript{80} \textit{Id.}

\textsuperscript{81} \textit{SS8 Networks}, \textit{supra} note 59, at 63–64.

\textsuperscript{82} \textit{Id.}

\textsuperscript{83} \textit{Id.}
Any restriction of this right shall be allowed only under an order of a court of law.\textsuperscript{84}

The 2003 Communications Law protects secrecy of communications, and requires a court order for wiretaps except as otherwise authorized by law.\textsuperscript{85} The Federal Security Service has not always required more than administrative approval for some wiretapping activities, especially if terrorism or national security is at issue.\textsuperscript{86} Thus, although protections somewhat parallel to the Fourth Amendment and Title III exist,\textsuperscript{87} it is unclear how closely agencies must adhere to them in practice.

F. China

There are limited rights to privacy in the Chinese Constitution. Article 38 states that the personal dignity of citizens of the People’s Republic of China is inviolable.\textsuperscript{88} Articles 37 and 39 define the protection of freedom of the person and the home.\textsuperscript{89} Article 40 provides for the freedom and privacy of correspondence.\textsuperscript{90} Warrants are required before a search, but this is often ignored, and the Public Security Bureau and prosecutors can issue warrants on their own authority, often without judicial oversight.\textsuperscript{91} The U.S. State Department reported, "During the year, authorities monitored telephone conversations, facsimile transmissions, e-mail, text-messaging, and Internet communications.... The security services routinely monitored and entered residences and offices."\textsuperscript{92} Information gained from a Chinese wiretap is thus unlikely to meet the requirements of the Fourth Amendment as applied within the United States.


\textsuperscript{86} Id.

\textsuperscript{87} For example, Russia is also a signatory to the European Convention for the Protection of Human Rights and Fundamental Freedoms. European Convention for the Protection of Human Rights and Fundamental Freedoms, Feb. 28, 1996, 213 U.N.T.S. 221.


\textsuperscript{89} XIAN FA, supra note 88, at arts. 37, 39.

\textsuperscript{90} Id. at art. 40.


\textsuperscript{92} Id.
III. Admission of Foreign Wiretap Evidence in United States Courts

United States federal courts have held that wiretap evidence obtained abroad is admissible in this country, even if obtained in a manner contrary to requirements in the United States. First, federal statutory law has no application outside United States territory unless a contrary intent is specifically indicated in the statute itself. No such intent is part of Title III. Second, the protections of the United States Constitution are much more limited abroad, although some Fourth Amendment protections do still remain in certain exceptional circumstances. As a result, courts have allowed information from foreign wiretaps into evidence even when the wiretapping would not have complied with Title III or the Fourth Amendment if performed within the United States. This follows from the general proposition that “all relevant evidence is admissible unless there is an exclusionary rule.”

A. Title III is Inapplicable Outside the United States

There is a “general canon of construction which teaches that, unless a contrary intent appears, federal statutes apply only within the territorial jurisdiction of the United States.” Federal courts have held specifically that Title III, the federal statute governing wiretapping and eavesdropping, has no application outside the United States and “significantly makes no provision for obtaining authorizations for a wiretap in a foreign country.”

In United States v. Peterson, the Ninth Circuit wrote, “Appellants also argue that the wiretap evidence should be excluded as violative of Title III. . . . We reject this argument. Title III has no extraterritorial force.”

93. See, e.g., United States v. Cotroni, 527 F.2d 708 (2d Cir. 1975) (federal wiretapping statute inapplicable to communications intercepted by Canadian officials in Canada, despite traveling in part over the U.S. communications system).

94. Id. at 711; see also Stowe v. Devoy, 588 F.2d 336, 341–42 (2d Cir. 1978); Foley Bros. v. Filardo, 336 U.S. 281, 285 (1949).


96. United States v. Barona, 56 F.3d 1087, 1091 (9th Cir. 1995) (quoting United States v. Maher, 645 F.2d 780, 782 (9th Cir. 1981)).

97. Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1968) (admitting evidence obtained during raids in the Philippines while saying, “If the raids had been conducted by United States agents, they would have been illegal under our Constitution.”).

98. Id. at 742.

99. United States v. Cotroni, 527 F.2d 708, 711 (2d Cir. 1975); see also Stowe, 588 F.2d at 341–42; Foley Bros., 336 U.S. at 285.

100. Toscanino, 500 F.2d at 279–80.

101. United States v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987) (citation omitted).
As a result, none of the statutory protections or requirements of Title III apply to wiretaps outside the territorial jurisdiction of the United States. Since much of the case law regarding admissibility and conduct of wiretaps revolves around the interpretation and application of Title III, this result changes the analysis of foreign wiretap evidence. Instead of relying primarily on statutory interpretation, such an analysis must instead focus on the transnational implications of the United States Constitution and, specifically, the Fourth Amendment.

B. The Fourth Amendment Provides Limited Protection Outside the United States

"As a starting point," wrote the Fifth Circuit in United States v. Morrow, "the Fourth Amendment exclusionary rule does not apply to arrests and searches made by foreign authorities on their home territory and in the enforcement of foreign law, even if the persons arrested and from whom the evidence is seized are American citizens." The Second Circuit notes that "information furnished to American officials need not be excluded simply because the procedures followed in securing it did not fully comply with our nation's constitutional requirements." Miranda warnings may be "overlooked" and "the lack of a proper search warrant may be disregarded."

However, the courts have been reluctant to remove all constitutional restrictions on wiretap evidence obtained abroad. Two "very limited exceptions" apply to the general proposition that "[n]either our Fourth Amendment nor the judicially-created exclusionary rule applies to acts of foreign officials." The first exception arises if the circumstances of the search are so extreme as to "shock the [judicial] conscience," in which case the courts can exclude the evidence improvidently obtained. The second exception is often referred to as the "Joint Venture Doctrine": if American officials "substantially participated" in the search or if foreign officials were acting as "agents" of American officials, courts may also exclude such evidence.

102. United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976); see also Stephen A. Saltzburg, The Reach of the Bill of Rights Beyond the Terra Firma of the United States, 20 VA. J. INT'l L. 741, 745-46 (1980).
103. Cotroni, 527 F.2d at 711.
104. Id. at 711-12.
105. United States v. Barona, 56 F.3d 1087, 1091 (9th Cir. 1995) (quoting United States v. Maher, 645 F.2d 780, 782 (9th Cir. 1981)).
106. Id.
1. Shocking the Conscience

While the courts have reserved the right to exclude evidence if the circumstances of a search and seizure are so extreme as to "shock the [judicial] conscience," the actual application of this doctrine is unclear. It is not enough, for example, that a wiretap is obtained "in violation of the foreign law itself" as the courts have "not excluded the evidence under this rationale." The First Circuit explains, "Circumstances that will shock the conscience are limited to conduct that 'not only violates U.S. notions of due process, but also violates fundamental international norms of decency.' Such fundamental norms may include those found, for example, in the Universal Declaration of Human Rights. One domestic case in which the Supreme Court did find "conduct that shocks the conscience" involved the forced pumping of a suspect's stomach to extract two morphine pills, later introduced as evidence. Generally, courts have been reluctant to find particular conduct, short of conduct approaching torture, to be so shocking as to require suppression.

2. Joint Ventures

Courts conduct a three-part analysis to determine the admissibility of evidence seized as part of a "joint venture": (1) is the participation of agents of the United States so substantial as to constitute a joint venture?; (2) if so, was foreign law complied with?; and, (3) if it was not, did U.S. agents act on a "reasonable belief that the foreign search complied with the foreign country's law?" First, was there substantial participation by agents of the United States? Under what is typically referred to as the "Joint Venture

108. Barona, 56 F.3d at 1091; see also United States v. Nagelberg, 434 F.2d 585, 587 n.1 (2d Cir. 1970) ("There is no claim of 'rubbing pepper in the eyes,' or other shocking conduct."); Birdsell v. United States, 346 F.2d 775, 782 n.10 (5th Cir 1965) ("We do not mean to say that in a case where federal officials had induced foreign police to engage in conduct that shocked the conscience, a federal court, in the exercise of its supervisory powers over the administration of federal justice, might not refuse to allow the prosecution to enjoy the fruits of such action.").

109. Barona, 56 F.3d at 1091 (citing United States v. Peterson, 812 F.2d 486, 491 (9th Cir. 1987)).

110. United States v. Mitro, 880 F.2d 1480, 1483–84 (quoting Saltzburg, supra note 102, at 775).

111. Saltzburg, supra note 102, at 775.

112. Rochin v. California, 342 U.S. 165, 172 (1951) ("[P]roceedings by which this conviction was obtained do more than offend some fastidious squeamishness or private sentimentalism about combating crime too energetically. This is conduct that shocks the conscience.").


114. United States v. Ferguson, 508 F. Supp. 2d 1, 2 (D.C. 2007) (citing United States v. Barona, 56 F.3d 1087, 1091 (9th Cir. 1995)).
Doctrine,"115 courts look to see "if American law enforcement officials substantially participated in the search or if the foreign officials conducting the search were actually acting as agents for their American counterparts."116 The doctrine is a "purposefully limited exception," and there is generally a "high threshold for a defendant to invoke it."117

Thus, in United States v. Ferguson, the district court found there was not a joint venture between the U.S. Drug Enforcement Administration ("DEA") and the Royal Bahamas Police Force ("RBPF") because (1) the RBPF initiated the investigation that included wiretaps; (2) the RBPF determined the scope and direction of the investigation; (3) DEA agents did not direct day-to-day activities; (4) DEA agents did not provide "substantial resources, such as the provision of translation and decoding services"; and, (5) DEA agents did not get immediate access to intercepted communications.118 Similarly, in United States v. Rosenthall, the court found no joint venture despite the presence of U.S. agents during a search of the defendant’s residence and briefings of the agents in advance by Columbian police.119 And again, in United States v. Maturo, the court found no joint venture, despite U.S. officials informing Turkish police of the defendant’s activities and reviewing tapes of the Turkish wiretap.120

On the other hand, in Peterson, the DEA informed the Philippines Narcotics Command of a suspected shipment bound for the United States via the Philippines.121 The Philippine authorities then initiated various wiretaps and intercepts.122 The DEA listened to tapes, "translated and decoded intercepted transmissions," and advised the Philippine authorities on relevancy.123 The DEA also referred to the operation as a "joint investigation."124 As a result, the Ninth Circuit held that there was a joint venture.125 In United States v. Barona, the DEA asked Danish police to place wiretaps, immediately obtained the information that resulted, and

115. Id. at 4.
118. Ferguson, 508 F. Supp. 2d at 5–6.
119. United States v. Rosenthall, 793 F.2d 1214, 1231 (11th Cir. 1986).
120. United States v. Maturo, 982 F.2d 57 (2d Cir. 1992).
121. United States v. Peterson, 812 F.2d 486, 488 (9th Cir. 1987).
122. Id. at 488–89.
123. Id. at 489–90.
124. Id. at 490.
125. Id.
provided an interpreter.\textsuperscript{126} This, said the Ninth Circuit, was also a joint venture.\textsuperscript{127}

Second, was foreign law complied with? The local law where the intercept occurred "governs whether the search was reasonable."\textsuperscript{128} Since "the touchstone of the Fourth Amendment is reasonableness,"\textsuperscript{129} "compliance with the foreign law alone determines whether the search violated the Fourth Amendment."\textsuperscript{130} The first step in answering this question requires determining what the foreign law is. This determination is a question of law "to be established by any relevant source, including testimony."\textsuperscript{131} The burden of defining foreign law currently rests with the defendant: "The burden is, of course, on the accused in the first instance to prove to the trial court's satisfaction that wire tapping was unlawfully employed."\textsuperscript{132}

In \textit{Peterson}, the Ninth Circuit examined two parts of Philippine law: the Philippine Constitution, which mirrors our Fourth Amendment in relevant part,\textsuperscript{133} and the Republic Act 4200,\textsuperscript{134} which governs wiretapping.\textsuperscript{135} Both sides conceded that "judicial authorization was neither sought nor received."\textsuperscript{136} The court noted, however, that there was a "public safety" exemption in the law.\textsuperscript{137} The court then looked for rulings by Philippine courts on the issue, but found little to go on, although noting that Philippine courts generally ruled in favor of individual liberties.\textsuperscript{138} In the end, the Ninth Circuit chose to decide the case "on the assumption that the search did not comply with Philippine law and was, as a result, not reasonable under the fourth amendment."\textsuperscript{139} In \textit{Barona}, also decided by the Ninth Circuit, the court looked to section 191 of the Danish Criminal Code.

\begin{thebibliography}{99}
\item 126. United States v. Barona, 56 F.3d 1087, 1094 (9th Cir. 1995).
\item 127. Id.
\item 128. \textit{Peterson}, 812 F.2d at 491.
\item 129. United States v. Purcell, 236 F.2d 1274, 1278 (11th Cir. 2001) (citing Ohio v. Robinetter, 519 U.S. 33, 39 (1996)); \textit{see also Barona}, 56 F.3d at 1093.
\item 130. \textit{Peterson}, 812 F.2d at 491.
\item 131. Id. at 490 (citing FED. R. CRIM. P. 26.1).
\item 133. CONST. (1987) Art. III, § 2, (Phil.).
\item 134. An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for other Purposes, Rep. Act No. 4200, (June 19, 1965) (Phil.); \textit{see also} United States v. Peterson, 812 F.2d 486, 491 (9th Cir. 1987).
\item 135. \textit{Peterson}, 812 F.2d at 491.
\item 136. Id.
\item 137. Id.
\item 138. Id.
\item 139. Id.
\end{thebibliography}
and sections 780 to 791 of the Danish Administration of Justice Act.\textsuperscript{140} They "carefully review[ed] the record" and, as a result, "[n]one of the evidence from the wiretaps is therefore subject to exclusion under the Fourth Amendment."\textsuperscript{141}

Third, if foreign law was not complied with, was the reliance by U.S. officials reasonable? This is the "good faith exception."\textsuperscript{142} The exception allows courts not to exclude evidence, even if foreign law was not complied with and even if the search was therefore unreasonable.\textsuperscript{143} The reliance by U.S. officials must be "objectively reasonable": "permitting reasonable reliance on representations about foreign law is a rational accommodation to the exigencies of foreign investigations."\textsuperscript{144} The Fifth Circuit explains, "The reasoning usually tendered in support of this limitation is the doubtful deterrent effect on foreign police practices that will follow from a punitive exclusion of the evidence in question by an American court."\textsuperscript{145}

In \textit{Stowe v. Devoy}, the appellant argued to the Second Circuit "that exclusion would deter further [foreign] intrusions upon the privacy of American citizens."\textsuperscript{146} But the court was not convinced: "[T]he exclusionary rule, as a deterrent sanction, is not applicable where a private party or a foreign government commits the offending act. Rather, the exclusionary rule is intended to inculcate a respect for the police of our own nation."\textsuperscript{147} In \textit{Peterson}, despite "assum[ing] that the search did not comply with Philippine law," the court decided that the "reliance in this case was objectively reasonable... federal officers sought, and received, assurances from high ranking law enforcement authorities in the Philippines that all necessary authorization was being obtained."\textsuperscript{148} In addition, the court said "search and seizure law in the Philippines is less than completely clear."\textsuperscript{149} And finally, to hold American officials "to a strict liability standard for failings of their foreign associates would be even more incongruous than holding law enforcement officials to a strict liability

\textsuperscript{140} United States v. Barona, 56 F.3d 1087, 1094 (9th Cir. 1995).
\textsuperscript{141} \textit{Id.} at 1096.
\textsuperscript{142} \textit{Peterson}, 812 F.2d at 492.
\textsuperscript{143} \textit{Id.}
\textsuperscript{144} \textit{Id.}
\textsuperscript{145} United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976); see also Brulay v. United States, 383 F.2d 345, 349 (9th Cir. 1967).
\textsuperscript{146} \textit{Stowe v. Devoy}, 588 F.2d 336, 341 n.13 (2d Cir. 1978).
\textsuperscript{147} \textit{Id.}
\textsuperscript{148} \textit{Peterson}, 812 F.2d at 492.
\textsuperscript{149} \textit{Id.}
standard as to the adequacy of domestic warrants.” 150 As a result, the court “conclude[d] that the good faith exception... applies to the foreign search” and allowed the evidence to be admitted. 151

C. Transnational Communications

Telephone calls and other communications regularly cross international boundaries, and it is not at all uncommon for one party in the United States to communicate with someone outside the country. Faced with this situation, courts have held that the fact that one party was in the United States during the wiretap intercept “does not change the result... . The law of the locality in which the tap exists (and where the interception takes place) governs its validity, even though the intercepted phone conversations traveled in part over the United States communication system.” 152 This follows, according to the United States v. Cotroni court, from the holding that “the federal statute governing wiretapping and eavesdropping [Title III]... has no application outside the United States.” 153

The courts have generally been comfortable allowing domestic wiretaps that unintentionally target other parties, provided Title III requirements are met. 154 Unnamed and unintended targets of a wiretap can contest the admissibility of the evidence under Title III, at least when it is to be used against them. 155 While based on Title III, the fundamental basis of these challenges is the Fourth Amendment itself, and the protections it provides against unreasonable search and seizure. 156 These same protections are not readily available when the wiretap is placed outside of the United States, but target—either intentionally or not—an individual within the United States.

Conclusion

As a result, there are two potential paths for transnational wiretaps to short-circuit the Fourth Amendment’s protections, even when the target is

150. Id.
151. Id.
152. Stowe, 588 F.2d at 341 n.12 (citing United States v. Cotroni, 527 F.2d 708, 711 (2d Cir. 1975)).
153. Id. at 341 n.12 (citing United States v. Toscanino, 500 F.2d 267, 270 (2d Cir. 1974)).
155. See id. § 2518(10)(a) (“Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter.”).
156. Boucher et al., supra note 13, at 5.
in the United States and is eventually prosecuted within the United States: (1) foreign wiretaps initiated by foreign governments without the direct involvement of the United States may produce results that can be used against U.S. defendants, regardless of what law was or was not followed, or (2) the United States may initiate or involve itself in a wiretap placed outside of the United States in cooperation with a foreign state. Both of these situations have the potential to seriously undermine Fourth Amendment protections. The first situation almost completely escapes constitutional and Fourth Amendment scrutiny unless the conduct involved rises to a level close to torture. The second situation allows for some constitutional scrutiny, but ultimately depends on the foreign law involved or, even if that was violated, whether U.S. officials reasonably relied on assurances by their foreign counterparts that the wiretap was conducted appropriately.

Actions by foreign agents without U.S. involvement are least amenable to Fourth Amendment scrutiny. Deterrence is the primary rationale for the exclusionary rule. 157 It is unlikely that foreign agents will be deterred from conduct that violates the U.S. Constitution if the United States is not even involved in the process until after the evidence is gathered. 158 In addition, "it is difficult to imagine that decisions of U.S. courts to admit evidence seized solely by foreign officers encourage abuse of foreign law." 159 There remains the real possibility that even greater cooperation between countries and officials may make it more and more likely that decisions by U.S. courts on evidence-gathering methods may indirectly influence foreign actions, but I do not believe we have yet reached the point where U.S. courts can legitimately judge foreign agents acting under foreign law with no involvement of U.S. officials. In addition, countries with which we are most connected, such as, for example, Canada, the United Kingdom, and Europe generally, are most likely to provide unsought evidentiary aid to our law enforcement agencies. Moreover, these countries are also most likely to observe similar safeguards to our own Fourth Amendment. In addition, actions by the judicial branch in this regard implicate separation of powers issues, and may be best left to the executive branch and the legislative branch to negotiate and pass treaties or influence foreign legislation to comport with our Fourth Amendment protections.

If American officials initiate or are substantially involved, however, the equation changes. There should be no benefit to U.S. agents to seek an

158. See Saltzburg, supra note 102, at 765.
159. Id.
end-run around constitutional protections, and the exclusionary rule—intended to foster respect for such protections—is perfectly suited for that end. As such, courts should do more than require a "good faith" effort by U.S. officials that foreign laws will be followed. They should also inquire as to whether or not the foreign law rises to a level substantially equivalent to our Fourth Amendment. At the very least, they should insist there has been a reasonable basis for the wiretap. If foreign laws are not sufficient, U.S. officials should insist on at least this minimum standard before initiating or actively participating in a wiretap. Such an inquiry should be made whenever foreign wiretap evidence, gathered as part of a "joint venture," is introduced into an American court, but it is especially critical to do so if the target—intended or not—is within the United States. Constitutional protections, after all, protect "people—and not simply areas"160 And to do so effectively, courts must act to prevent an end-run around the Fourth Amendment.
