Law, Crime and Law Enforcement

LAUREL JENNINGS
RICHARD M. EASTMAN
EDITORS

WIRETAPS AND ELECTRONIC EAVESDROPPING

Federal Law and Legal Ethics

NOVA

LAW, CRIME AND LAW ENFORCEMENT

WIRETAPS AND ELECTRONIC EAVESDROPPING

FEDERAL LAW AND LEGAL ETHICS

LAUREL JENNINGS
AND
RICHARD M. EASTMAN
EDITORS

nova publishers
New York

Library of Congress Cataloging-in-Publication Data

ISBN: 978-1-62257-992-1

Published by Nova Science Publishers, Inc. † New York

LAW, CRIME AND LAW ENFORCEMENT

WIRETAPS AND ELECTRONIC EAVESDROPPING

FEDERAL LAW AND LEGAL ETHICS

LAW, CRIME AND LAW ENFORCEMENT

Additional books in this series can be found on Nova's website
under the Series tab.

Additional E-books in this series can be found on Nova's website
under the E-book tab.

PRIVACY AND IDENTITY PROTECTION

Additional books in this series can be found on Nova's website
under the Series tab.

Additional E-books in this series can be found on Nova's website
under the E-book tab.

PREFACE

It is a federal crime to wiretap or to use a machine to capture the communications of others without court approval, unless one of the parties has given his prior consent. It is likewise a federal crime to use or disclose any information acquired by illegal wiretapping or electronic eavesdropping. Violations can result in imprisonment for not more than five years; fines up to $250,000; in civil liability for damages, attorney's fees and possibly punitive damages; in disciplinary action against any attorneys involved; and in suppression of any derivative evidence. This book provides an overview of federal law governing wiretapping and electronic eavesdropping under the Electronic Communications Privacy Act (ECPA).

Chapter 1 – This report provides an overview of federal law governing wiretapping and electronic eavesdropping under the Electronic Communications Privacy Act (ECPA). It also appends citations to state law in the area and the text of ECPA.

It is a federal crime to wiretap or to use a machine to capture the communications of others without court approval, unless one of the parties has given his prior consent. It is likewise a federal crime to use or disclose any information acquired by illegal wiretapping or electronic eavesdropping. Violations can result in imprisonment for not more than five years; fines up to $250,000 (up to $500,000 for organizations); in civil liability for damages, attorneys' fees and possibly punitive damages; in disciplinary action against any attorneys involved; and in suppression of any derivative evidence. Congress has created separate, but comparable, protective schemes for electronic communications (e.g., email) and against the surreptitious use of telephone call monitoring practices such as pen registers and trap and trace devices.

Each of these protective schemes comes with a procedural mechanism to afford limited law enforcement access to private communications and communications records under conditions consistent with the dictates of the Fourth Amendment. The government has been given narrowly confined authority to engage in electronic surveillance, conduct physical searches, and install and use pen registers and trap and trace devices for law enforcement purposes under ECPA and for purposes of foreign intelligence gathering under the Foreign Intelligence Surveillance Act.

Chapter 2 – In some jurisdictions, it is unethical for an attorney to secretly record a conversation even though it is not illegal to do so. A few states require the consent of all parties to a conversation before it may be recorded. Recording without mutual consent is both illegal and unethical in those jurisdictions. Elsewhere the matter is more uncertain.

In 1974, the American Bar Association (ABA) opined that surreptitiously recording a conversation without the knowledge or consent of all of the participants violated the ethical prohibition against engaging in conduct involving "dishonesty, fraud, deceit or misrepresentation." The ABA conceded, however, that law enforcement recording, conducted under judicial supervision, might breach no ethical standard. Reaction among the authorities responsible for regulation of the practice of law in the various states was mixed. In 2001, the ABA reversed its earlier opinion and announced that it no longer considered one-party consent recording per se unethical when it is otherwise lawful.

Today, this is the view of a majority of the jurisdictions on record. A substantial number, however, disagree. An even greater number have yet announce to an opinion.

A sampling of the views of various bar associations in the question is attached. An earlier version of this report once appeared under the same title as CRS Report 98-250. An abridged version of this report is available without footnotes or attachment as CRS Report R42649, Wiretapping, Tape Recorders, and Legal Ethics: An Abridged Overview of Questions Posed by Attorney Involvement in Secretly Recording Conversation.

CONTENTS

Preface		**vii**
Chapter 1	Privacy: An Overview of the Electronic Communications Privacy Act *Charles Doyle*	**1**
Chapter 2	Wiretapping, Tape Recorders, and Legal Ethics: An Overview of Questions Posed by Attorney Involvement in Secretly Recording Conversation *Charles Doyle*	**135**
Index		**171**

In: Wiretaps and Electronic Eavesdropping ISBN: 978-1-62257-992-1
Editors: L. Jennings and R. M. Eastman

Chapter 1

PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT*

Charles Doyle

SUMMARY

This report provides an overview of federal law governing wiretapping and electronic eavesdropping under the Electronic Communications Privacy Act (ECPA). It also appends citations to state law in the area and the text of ECPA.

It is a federal crime to wiretap or to use a machine to capture the communications of others without court approval, unless one of the parties has given his prior consent. It is likewise a federal crime to use or disclose any information acquired by illegal wiretapping or electronic eavesdropping. Violations can result in imprisonment for not more than five years; fines up to $250,000 (up to $500,000 for organizations); in civil liability for damages, attorneys' fees and possibly punitive damages; in disciplinary action against any attorneys involved; and in suppression of any derivative evidence. Congress has created separate, but comparable, protective schemes for electronic communications (e.g., email) and against the surreptitious use of telephone call monitoring practices such as pen registers and trap and trace devices.

* This is an edited, reformatted and augmented version of a Congressional Research Service publication, CRS Report for Congress R41733, from www.crs.gov, dated March 30, 2011.

Each of these protective schemes comes with a procedural mechanism to afford limited law enforcement access to private communications and communications records under conditions consistent with the dictates of the Fourth Amendment. The government has been given narrowly confined authority to engage in electronic surveillance, conduct physical searches, and install and use pen registers and trap and trace devices for law enforcement purposes under ECPA and for purposes of foreign intelligence gathering under the Foreign Intelligence Surveillance Act.

INTRODUCTION

Depending on one's perspective, wiretapping and electronic eavesdropping are either "dirty business," essential law enforcement tools, or both. This is a very general overview of the federal statutes that proscribe wiretapping and electronic eavesdropping and of the procedures they establish for law enforcement purposes. Although the specifics of state law are beyond the scope of this report, citations to related state statutory provisions have been appended. The text of pertinent federal statutes appears as an appendix as well.[1]

BACKGROUND

At common law, "eavesdroppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet; or are indictable at the sessions, and punishable by fine and finding of sureties for [their] good behavior."[2] Although early American law proscribed common law eavesdropping, the crime was little prosecuted and by the late nineteenth century had "nearly faded from the legal horizon."[3] With the invention of the telegraph and telephone, however, state laws outlawing wiretapping or indiscretion by telephone and telegraph operators preserved the spirit of the common law prohibition in this country.

Congress enacted the first federal wiretap statute as a temporary measure to prevent disclosure of government secrets during World War I.[4] Later, it proscribed intercepting and divulging private radio messages in the Radio Act of 1927,[5] but did not immediately reestablish a federal wiretap prohibition. By the time of the landmark Supreme Court decision in *Olmstead*, however, at

least forty-one of the forty-eight states had banned wiretapping or forbidden telephone and telegraph employees and officers from disclosing the content of telephone or telegraph messages or both.[6]

Olmstead was a Seattle bootlegger whose Prohibition Act conviction was the product of a federal wiretap. He challenged his conviction on three grounds, arguing unsuccessfully that the wiretap evidence should have been suppressed as a violation of either his Fourth Amendment rights, his Fifth Amendment privilege against self-incrimination, or the rights implicit in the Washington state statute that outlawed wiretapping.

For a majority of the Court, writing through Chief Justice Taft, Olmstead's Fourth Amendment challenge was doomed by the absence of "an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house or curtilage[7] for the purposes of making a seizure."[8]

Chief Justice Taft pointed out that Congress was free to provide protection which the Constitution did not.[9] Congress did so in the 1934 Communications Act by expanding the Radio Act's proscription against intercepting and divulging radio communications so as to include intercepting and divulging radio or wire communications.[10]

The Federal Communications Act outlawed wiretapping, but it said nothing about the use of machines to surreptitiously record and transmit face to face conversations.[11] In the absence of a statutory ban the number of surreptitious recording cases decided on Fourth Amendment grounds surged and the results began to erode *Olmstead*'s underpinnings.[12]

Erosion, however, came slowly. Initially the Court applied *Olmstead*'s principles to the electronic eavesdropping cases. Thus, the use of a dictaphone to secretly overhear a private conversation in an adjacent office offended no Fourth Amendment precepts, because no physical trespass into the office in which the conversation took place had occurred.[13] Similarly, the absence of a physical trespass precluded Fourth Amendment coverage of the situation where a federal agent secretly recorded his conversation with a defendant held in a commercial laundry in an area open to the public.[14] On the other hand, the Fourth Amendment did reach the government's physical intrusion upon private property during an investigation, as for example when they drove a "spike mike" into the common wall of a row house until it made contact with a heating duct for the home in which the conversation occurred.[15]

The spike mike case presented something of a technical problem, because there was some question whether the spike mike had actually crossed the property line of the defendant's town house when it made contact with the

heating duct. The Court declined to rest its decision on the technicalities of local property law, and instead found that the government's conduct had intruded upon privacy of home and hearth in a manner condemned by the Fourth Amendment.[16]

Each of these cases focused upon whether a warrantless trespass onto private property had occurred, that is, whether the *means* of conducting a search and seizure had been so unreasonable as to offend the Fourth Amendment. Yet in each case, the object of the search and seizure had been not those tangible papers or effects for which the Fourth Amendment's protection had been traditionally claimed, but an intangible, a conversation. This enlarged view of the Fourth Amendment could hardly be ignored, for "[i]t follows from . . . *Silverman* . . . that the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of papers and effects."[17]

Soon thereafter the Court repudiated the notion that the Fourth Amendment's protection was contingent upon some trespass to real property in *Katz v. United States.*[18] Katz was a bookie convicted on the basis of evidence gathered by an electronic listening and recording device set up outside the public telephone booth that Katz used to take and place bets. The Court held that the gateway for Fourth Amendment purposes stood at that point where an individual should to able to expect that his or her privacy would not be subjected to unwarranted governmental intrusion.[19]

One obvious consequence of Fourth Amendment coverage of wiretapping and other forms of electronic eavesdropping is the usual attachment of the Amendment's warrant requirement. To avoid constitutional problems and at the same time preserve wiretapping and other forms of electronic eavesdropping as a law enforcement tool, some of the states established a statutory system under which law enforcement officials could obtain a warrant, or equivalent court order, authorizing wiretapping or electronic eavesdropping.

The Court rejected the constitutional adequacy of one of the more detailed of these state statutory schemes in *Berger v. New York.*[20] The statute was found deficient because of its failure to require:

- a particularized description of the place to be searched;
- a particularized description of the crime to which the search and seizure related;
- a particularized description of the conversation to be seized;
- limitations to prevent general searches;

- termination of the interception when the conversation sought had been seized;
- prompt execution of the order;
- return to the issuing court detailing the items seized; and
- any showing of exigent circumstances to overcome the want of prior notice.[21]

Berger helped persuade Congress to enact Title III of the Omnibus Crime Control and Safe Streets Act of 1968, a comprehensive wiretapping and electronic eavesdropping statute that not only outlawed both activities in general terms but that also permitted federal and state law enforcement officers to use them under strict limitations designed to meet the objections in Berger.[22]

A decade later another Supreme Court case persuaded Congress to supplement Title III with a judicially supervised procedure for the use of wiretapping and electronic eavesdropping in foreign intelligence gathering situations. When Congress passed Title III there was some question over the extent of the President's inherent powers to authorize wiretaps – without judicial approval – in national security cases. As a consequence, the issue was simply removed from the Title III scheme.[23] After the Court held that the President's inherent powers were insufficient to excuse warrantless electronic eavesdropping on purely domestic threats to national security,[24] Congress considered it prudent to augment the foreign intelligence gathering authority of the United States with the Foreign Intelligence Security Act of 1978 (FISA).[25] The FISA provides a procedure for judicial review and authorization or denial of wiretapping and other forms of electronic eavesdropping for purposes of foreign intelligence gathering.

Two other Supreme Court cases influenced the development of federal law in the area. In United States v. Miller,[26] the Court held that a customer had no Fourth Amendment protected expectation of privacy in the records his bank created concerning his transactions with them. These third party records were therefore available to the government under a subpoena duces tecum rather than a more narrowly circumscribed warrant.[27] In Smith v. Maryland,[28] it held that no warrant was required for the state's use of a pen register or trap and trace device, if the device merely identified the telephone numbers for calls made and received from a particular telephone. No Fourth Amendment search or seizure occurred, the Court held, since the customer had no justifiable expectation of privacy in information which he knew or should have known

the telephone company might ordinarily capture for billing or service purposes.[29]

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA).[30] ECPA consists of three parts: a revised Title III;[31] the Stored Communications Act (SCA);[32] and provisions governing the installation and use of trap and trace devices.[33]

TITLE III: PROHIBITIONS

Unless otherwise provided, Title III outlaws wiretapping and electronic eavesdropping; possession of wiretapping or electronic eavesdropping equipment; use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping; and disclosure of information secured through court-ordered wiretapping or electronic eavesdropping, in order to obstruct justice, 18 U.S.C. 2511. Elsewhere, federal law proscribes:

- unlawful access to stored communications, 18 U.S.C. 2701;
- unlawful use of a pen register or a trap and trace device, 18 U.S.C. 3121; and
- abuse of eavesdropping and search authority or unlawful disclosures under the Foreign Intelligence Surveillance Act, 50 U.S.C. 1809, 1827.

Illegal Wiretapping and Electronic Eavesdropping

At the heart of Title III lies the prohibition against illegal wiretapping and electronic eavesdropping, 18 U.S.C. 2511(1), that bans:

- any person from
- intentionally
- intercepting, or endeavoring to intercept,
- wire, oral or electronic communications
- by using an electronic, mechanical or other device
- unless the conduct is specifically authorized or expressly not covered, *e.g.*
  - one of the parties to the conversation has consented to the interception

- the interception occurs in compliance with a statutorily authorized, (and ordinarily judicially supervised) law enforcement or foreign intelligence gathering interception,
- the interception occurs as part of providing or regulating communication services,
- certain radio broadcasts, and
- in some places, spousal wiretappers.

Person

The prohibition applies to "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."[34]

Intentional

Conduct can only violate Title III if it is done "intentionally," inadvertent conduct is no crime; the offender must have done on purpose those things which are outlawed.[35] He need not be shown to have known, however, that his conduct was unlawful.[36]

Jurisdiction

Subsection 2511(1) contains two interception bars – one, 2511(1)(a), simply outlaws intentional interception; the other, 2511(1)(b), outlaws intentional interception when committed under any of five jurisdictional circumstances with either an implicit or explicit nexus to interstate or foreign commerce.[37] Congress adopted the approach because of concern that its constitutional authority might not be sufficient to ban instances of electronic surveillance that bore no discernable connection to interstate commerce or any other of Congress's enumerated constitutional powers. So it enacted a general prohibition, and as a safety precaution, a second provision more tightly tethered to specific jurisdictional factors.[38] The Justice Department has honored that caution by employing subparagraph (b) to prosecute the interception of oral communications, while using subparagraph (a) to prosecute other forms of electronic eavesdropping.[39]

Interception

Interception "means the aural or other acquisition of the contents" of various kinds of communications by means of "electronic, mechanical or other devices."[40] Although logic might suggest that interception occurs only in the place where the communication is captured, the cases indicate that interception

occurs as well where the communication begins, is transmitted, or is received.[41] Yet, it does not include instances when an individual simply reads or listens to a previously intercepted communication, regardless of whether additional conduct may implicate the prohibitions on use or disclosure.[42]

Once limited to aural acquisitions, ECPA enlarged the definition of "interception" by adding the words "or other acquisition" so that it is no longer limited to interceptions of communications that can be heard.[43] The change complicates the question of whether the wiretap, stored communications, or trap and trace portions of the ECPA govern the legality of various means of capturing information relating to a communication. The analysis might seem to favor wiretap coverage when it begins with an examination of whether an "interception" has occurred. Yet, there is little consensus over when an interception occurs; that is, whether "interception" as used in section 2511 contemplates surreptitious acquisition, either contemporaneous with transmission, or whether such acquisition may occur anytime before the initial cognitive receipt of the contents by the intended recipient, or under some other conditions.[44]

The USA PATRIOT Act resolved some of the statutory uncertainty concerning voice mail when it removed voice mail from the wiretap coverage of Title III (striking the phrase "and such term includes any electronic storage of such communication" from the definition of "wire communications" in Title III (18 U.S.C. 2510(1)) and added stored *wire* communications to the stored communications coverage of 18 U.S.C. 2703.[45]

Content

The interceptions proscribed in Title III are confined to those that capture a communication's "content," that is, "information concerning [its] substance, purport, or meaning."[46] Trap and trace devices and pen registers once captured only information relating to the source and addressee of a communication, not its content. That is no longer the case. The "post-cut-through dialed digit features" of contemporary telephone communications now transmit communications in such a manner that the use of ordinary pen register or trap and trace devices will capture both non-content and content.[47] As a consequence, a few courts have held, either as a matter of statutory construction or constitutional necessity, that the authorities must rely on a Title III wiretap order rather than a pen register/trap and trace order if such information will be captured.[48]

By Electronic, Mechanical, or Other Device

The statute does not cover common law "eavesdropping," but only interceptions "by electronic, mechanical or other device."[49] The term includes computers,[50] but it is defined so as not to include hearing aids or extension telephones in normal use (use in the "ordinary course of business").[51] Whether an extension phone has been installed and is being used in the ordinary course of business or in the ordinary course of law enforcement duties, so that it no longer constitutes an interception device for purposes of Title III and comparable state laws has proven a somewhat vexing question.[52]

Although often intertwined with the consent exception discussed below, the question generally turns on the facts in a given case.[53] When the exemption is claimed as a practice in the ordinary course of business, the interception must be for a legitimate business reason, it must be routinely conducted, and at least in some circuits employees must be notified that their conversations are being monitored.[54] Similarly, "Congress most likely carved out an exception for law enforcement officials to make clear that the routine and almost universal recording of phone lines by police departments and prisons, as well as other law enforcement institutions, is exempt from the statute."[55] The exception contemplates administrative rather than investigative monitoring,[56] which must nevertheless be justified by a lawful, valid law enforcement concern.[57]

Wire, Oral, or Electronic Communications

An interception can only be a violation of ECPA if the conversation or other form of communication intercepted is among those kinds which the statute protects, in oversimplified terms – telephone (wire), face to face (oral), and computer (electronic). Thus, silent video surveillance is ordinarily considered beyond ECPA's reach.[58]

Congress used the definitions of the three forms of communications to describe other communications beyond the ECPA's reach as well as those within its grasp. For example, "oral communication" by definition includes only those face to face conversations with respect to which the speakers have a justifiable expectation of privacy.[59] Similarly, "wire communications" are limited to those that are at some point involve voice communications (i.e., only aural transfers).[60] Radio and data transmissions are generally "electronic communications." The definition includes other forms of information transfer but excludes certain radio transmissions which can be innocently captured without great difficulty.[61] Although it is not a federal crime to intercept radio communications under any number of conditions, the exclusion is not a matter