# TABLE OF CONTENTS

TABLE OF CONTENTS .................................................................................................................. 1
INTRODUCTION .......................................................................................................................... 2
THEMES OF THE BOOK ............................................................................................................. 3
STRUCTURING THE COURSE ..................................................................................................... 5

## CHAPTER 1 PRIVACY AND LAW ENFORCEMENT ...... ERROR! BOOKMARK NOT DEFINED.

A. THE FOURTH AMENDMENT AND EMERGING TECHNOLOGY ERROR! BOOKMARK NOT DEFINED.

1. How The Fourth Amendment Works .................................................................................... Error! Bookmark not defined.
2. Wiretapping, Bugging, and Beyond ..................................................................................... Error! Bookmark not defined.
3. The Reasonable Expectation of Privacy Test ....................................................................... Error! Bookmark not defined.
   (a) The Third Party Doctrine ............................................................................................... Error! Bookmark not defined.
   (b) Items Abandoned or Exposed to the Public ................................................................. Error! Bookmark not defined.
   (c) Surveillance and the Use of Sense Enhancement Technologies ................................ Error! Bookmark not defined.
B. INFORMATION GATHERING ABOUT FIRST AMENDMENT ACTIVITIES ................. ERROR!

BOOKMARK not defined.

C. FEDERAL ELECTRONIC SURVEILLANCE LAW ........ ERROR! BOOKMARK not defined.

1. Section 605 of the Federal Communications Act ............................................................... Error! Bookmark not defined.
2. Title III ................................................................................................................................... Error! Bookmark not defined.
3. Electronic Communications Privacy Act ............................................................................. Error! Bookmark not defined.
4. The Communications Assistance for Law Enforcement Act ........................................... Error! Bookmark not defined.
5. The USA-PATRIOT Act ......................................................................................................... Error! Bookmark not defined.

D. DIGITAL SEARCHES AND SEIZURES .............................................................................. ERROR! BOOKMARK not defined.

2. Encryption ............................................................................................................................. Error! Bookmark not defined.
4. Email ..................................................................................................................................... Error! Bookmark not defined.
5. ISP Account Information ...................................................................................................... Error! Bookmark not defined.
6. IP Addresses, URLs, and Internet Searches ...................................................................... Error! Bookmark not defined.

## CHAPTER 2 NATIONAL SECURITY AND FOREIGN INTELLIGENCE ERROR! BOOKMARK NOT DEFINED.

A. THE INTELLIGENCE COMMUNITY ................................................................................. ERROR! BOOKMARK not defined.
B. THE FOURTH AMENDMENT FRAMEWORK .................................................................... ERROR! BOOKMARK not defined.
C. FOREIGN INTELLIGENCE GATHERING ............................................................................. ERROR! BOOKMARK not defined.

1. The Foreign Intelligence Surveillance Act ............................................................................. Error! Bookmark not defined.
2. The USA PATRIOT Act ........................................................................................................ Error! Bookmark not defined.
4. Internal Oversight ................................................................................................................ Error! Bookmark not defined.
   (a) The Attorney General’s FBI Guidelines ........................................................................... Error! Bookmark not defined.
   (b) The Homeland Security Act .......................................................................................... Error! Bookmark not defined.
   (c) The Intelligence Reform and Terrorism Prevention Act .............................................. Error! Bookmark not defined.
D. NSA SURVEILLANCE .......................................................................................................... ERROR! BOOKMARK not defined.

1. Standing ................................................................................................................................. Error! Bookmark not defined.
2. The Snowden Revelations .................................................................................................... Error! Bookmark not defined.
INTRODUCTION

OVERVIEW

The casebook is designed to provide reading material to cover the privacy issues involved in law enforcement and national security. It can also be used for seminars exploring a narrower subset of issues.

WEBSITE, NEW EDITIONS, AND COMMENTS

We have an extensive website to provide further resources for the casebook:

http://informationprivacylaw.com

On our website, we offer an update to our casebook each year, which can be downloaded for free. We provide links to useful blogs and websites pertaining to privacy law. We provide a list of recommended books that instructors might want to assign in their classes.

We hope that you visit and use our website. We are constantly working to improve it, and we welcome any suggestions you might have about it.

We welcome your suggestions for improving the casebook. Many of our changes in this edition and in the last one were based on comments by instructors. We believe the book grows stronger with each edition, and that is in part due to your help. Please feel free to contact either of us with your thoughts about the book:

Daniel J. Solove: dsolove@law.gwu.edu

Paul M. Schwartz: pschwartz@law.berkeley.edu
THEMES OF THE BOOK

A Body of Law in Development. Information privacy law is relatively youthful. It is still fresh from the mold and is quite malleable. One of the fascinating aspects of an information privacy class is focusing on how law responds to new situations brought about by new technologies, business practices, and government policies.

The Concept of Privacy. Underpinning almost all cases and statutes about privacy is a particular conception of privacy. Often the underlying concept is not made explicit. But information privacy law depends upon the concept of privacy. The cases and statutes adopt different views about privacy and what it entails. Privacy is an immensely complicated concept, and the course will frequently involve discussions about what privacy is and whether the particular conception underpinning a case or statute is appropriate.

Policy. Information privacy law is a course involving a great amount of policy. For many students this dimension provides an opportunity to explore the role of law prospectively. In addition to exploring privacy as the adjudication of particular disputes brought before a court, the text also looks at the development of privacy laws through the acts of legislatures and the directives and guidelines of international organizations.

Competing Interests. Few would assert that privacy is an absolute value. Many important interests come into conflict with privacy, such as freedom of speech and press, public safety, transparency, efficient economic transactions, and so on. Privacy also can further many of these interests as well. For example, protection against the disclosure of a telephone communication can inhibit speech (by preventing speech about the particular conversation), but it can also protect speech (by promoting telephone conversations in general). Privacy issues are rarely easy, and class discussions will often become spirited debates about the costs and benefits of protecting privacy in a particular context. The issue of public safety looms especially large post-9/11.

Reasonable Expectation of Privacy. Modern Fourth Amendment jurisprudence rests on the notion that we have expectations of privacy and that the law should protect those that society recognizes as reasonable. The notion of reasonable expectation of privacy is also frequently used in other areas of law, such as the privacy torts. What can we reasonably expect to be private? How are we to determine what expectations society should recognize as reasonable?

Privacy and Technology. New technology can provide new avenues for the protection of privacy (e.g., encryption and techniques for anonymization). It can also pose serious threats to privacy. How should the law grapple with regulating new technology? And critically how does the introduction of new technology change our understanding of the right of privacy – if at all?
Creative Lawyering. Because privacy is such a complicated and fresh issue, because the law is still in a state of rapid development, and because so many different areas of law come to bear on privacy problems, the course demands that students think creatively. Even if students don’t practice information privacy law later as attorneys, they will learn a valuable set of skills: how to see analogies between cases, how to distinguish cases, how to recognize the philosophical issues that underpin a case, how to recognize inconsistencies in the law and think of ways to resolve them, how to assess the way in which the law will respond to a new problem and novel issue, how to connect different areas of the law, how to draw from one area of law and import its concepts into a different area of law. Students should also consider the relationship between technology and law and the role of various legal institutions in responding to the challenge of new technology.

The Role of the Courts and the Legislature. The development of privacy law in the United States may also be viewed as a dialogue between the courts and the legislature about the scope and application of the legal concept of privacy. In some matters, courts will define new privacy rights. In others, the courts will leave the job to the legislature. An often recurring theme is whether the courts or the legislatures are best placed to define the right of privacy.
The casebook is designed for flexibility. It can be used in 2-credit seminars as well as supplemental reading for 3- or 4-credit courses.

The class hours below are recommendations. Instructors vary significantly on how much time they spend with particular material.

<table>
<thead>
<tr>
<th>TOPIC &amp; ASSIGNMENT</th>
<th>CLASS HOURS</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Privacy and Law Enforcement</td>
<td>3-4 hours</td>
<td>The wiretapping and audio surveillance materials cover <em>Katz</em> and the cases leading up to it. This material takes at least 1.5 to 2 hours. The material involving the application of the reasonable expectation of privacy test is very important and takes a minimum of 1.5 to 2 hours to cover.</td>
</tr>
<tr>
<td>A. The Fourth Amendment and Emerging Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Information Gathering About First Amendment Activities</td>
<td>½ hour</td>
<td>The material in this brief section can be covered quickly, though it can also lead to some fascinating discussions about how government searches and surveillance affect First Amendment rights.</td>
</tr>
<tr>
<td>C. Federal Electronic Surveillance Law</td>
<td>0- 1½ hours</td>
<td>The material in this part is mostly an expository introduction to the Electronic Communications Privacy Act (ECPA). It traces the history of electronic surveillance law and provides background about understanding the nuts and bolts about how ECPA works. This part is intended to give students a background about ECPA so students can better understand the cases in Part D.</td>
</tr>
<tr>
<td>D. Digital Searches and Seizures</td>
<td>3 hours</td>
<td>This part contains cases that apply ECPA and the Fourth Amendment to searches and seizures of digital information in computers and ISP records.</td>
</tr>
<tr>
<td>2. National Security and Foreign Intelligence</td>
<td>½ - 1 hour</td>
<td>The <em>Keith</em> case is a central case and should be covered in depth.</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>A. The Intelligence Community</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. The Fourth Amendment Framework</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Foreign Intelligence Gathering</td>
<td>1-2 hours</td>
<td>The material here focuses on FISA, and coverage time can vary depending upon how much depth instructors want to spend on the mechanics of FISA.</td>
</tr>
<tr>
<td>D. NSA Surveillance</td>
<td>1-2 hours</td>
<td>The <em>Clapper</em> case raises fundamental issues about defining privacy harms and can lead to a fruitful lengthy discussion. <em>Klayman</em> and <em>In re FBI</em> present starkly different applications of some of the Fourth Amendment doctrine covered in Chapter 4.</td>
</tr>
</tbody>
</table>
CHAPTER 1
PRIVACY AND LAW ENFORCEMENT

SUMMARY OF MAJOR CHANGES FROM THE PREVIOUS EDITION

• In Section D.1, after Andrus, a note was added to discuss Microsoft Corp. v. United States (Microsoft Ireland), 829 F.3d 197 (2d Cir. July 14, 2016).

A. THE FOURTH AMENDMENT AND EMERGING TECHNOLOGY

1. HOW THE FOURTH AMENDMENT WORKS

This section introduces the basic concepts of the Fourth and Fifth Amendments, with a particular focus on the Fourth Amendment. It explains, in turn, the applicability of the Fourth Amendment, the question of a search or seizure’s reasonableness, and enforcement of the Fourth Amendment.

2. WIRETAPPING, BUGGING, AND BEYOND

Chapter 4 begins its coverage of the Fourth Amendment by tracing the application of the Fourth Amendment to wiretapping. There is a central progression from Olmstead through Katz that helps establish several of the major themes in information privacy law, including the application of the Fourth Amendment to new technology, the role of the courts and the legislature, and the articulation of the reasonable expectation of privacy analysis.

It may be helpful at the outset to distinguish between the different ways that law enforcement officials can obtain information about a conversation. First, a party to the conversation can breach confidentiality and inform the police of what was said. Second, a police officer can eavesdrop by listening in on a conversation with the naked ear. Third, a police officer can pose as one’s friend (undercover agent) or the police can have an undercover informant to be a party to the conversation. Fourth, the undercover agent or informant can be bugged or “wired” with an electronic recording or transmitting device. Fifth, a bug can be installed at a particular location to pick up a conversation. Sixth, the police can wiretap the telephone lines and listen in on a telephone conversation.

Olmstead v. United States

Olmstead involves the first Fourth Amendment challenge to wiretapping. The Court holds that the Fourth Amendment doesn’t apply to wiretapping because there is no physical
trespass to the home. This holding is overruled in *Katz v. United States*. The enduring part of *Olmstead* is Justice Brandeis’s dissent.

There is much in the *Olmstead* opinion to explore. Central to the Court’s analysis is the question of whether the Fourth Amendment applies to searches that take place in the “ether.” Chief Justice Taft emphasizes the requirement of physical trespass in the Fourth Amendment. But note that the Court does not preclude the possibility that Congress could regulate this new form of search by legislative means.

**Note 1 – Background and Epilogue**

This note presents some interesting background information about Roy Olmstead, the “King of Bootleggers,” as well as about what happened in his trial and afterwards.

**Note 2 – The Physical Trespass Doctrine, Detectaphones, and “Spike Mikes”**

*Goldman v. United States* follows the reasoning of *Olmstead* and concludes that placing a microphone next to a wall adjacent to a person’s office does not invoke the protection of the Fourth Amendment because there was no physical trespass.

*Silverman v. United States* is another case that is based on the *Olmstead* notion of physical trespass. Here, the Court concludes that a microphone inserted into a baseboard and making contact with a home’s heating duct violated the Fourth Amendment because there was a physical trespass. The case differs from *Goldman* because there was a physical penetration into the home.

**Note 3 – Brandeis’s Dissent and the Warren and Brandeis Article**

This note asks students to compare the reasoning of Justice Brandeis’s dissent to his article with Samuel Warren, *The Right to Privacy* (Chapter 1). In that article, Warren & Brandeis argued that the “right to be let alone” was an overarching principle in the common law. In his *Olmstead* dissent Brandeis argues that the “right to be let alone” is also an overarching principle in constitutional law. Brandeis urges a common law style of reasoning when interpreting the Constitution.

**Note 4 – Changing Technology and the Constitution**

This note traces the idea of the need for a physical trespass for a Fourth Amendment violation. It looks at two later cases, *Goldman v. U.S.* (1942), and *Silverman v. U.S.* (1961).

**Note 5 – Wiretapping vs. Mail Tampering**

Brandeis’s comparison of a search of the mails with the interception of telephone communications is particularly illuminating and can help launch a discussion about the expectation of privacy in the Internet era. Note in particular Brandeis’s focus on the unbounded nature of the search in space and time that occurs in the electronic environment.
This issue reemerges in *Berger v. New York*, and then in the crafting of federal electronic surveillance law.

**Note 6 – State Wiretapping Law**

At the time of *Olmstead*, the state of Washington prohibited wiretapping. In dissent in *Olmstead*, Justice Holmes objected to this violation of law and argued that apart from the Fourth Amendment question, “the government ought not to use evidence obtained and only obtainable by a criminal act.” Should federal law enforcement officials be allowed to violate state criminal law when investigating suspects? The question raises issues of federal versus state power. If federal officials must be bound by state criminal law, then a state could criminalize many techniques and avenues for federal officials to investigate and enforce federal law. This might happen in circumstances where a state disagrees with a federal law, such as states that desire different rules for allowing the use of medical marijuana. On the other hand, allowing federal officials to ignore state criminal law provides them with a vast power against the states.

**Note 7 – The Birth of Federal Electronic Surveillance Law**

In reaction to *Olmstead*, Congress enacted a statute that made wiretapping a federal crime. We return to this statute in the section of this Chapter on electronic surveillance law; suffice it to say at this juncture, that § 605 of the Federal Communications Act proved to be notably ineffective.

**Note 8 – Secret Agents and Misplaced Trust**

This note introduces two cases, *Hoffa v. United States* and *Lewis v. United States*, which hold that the Fourth Amendment does not apply to undercover agents. The rationale of these cases is that when one person says something to another, that person assumes the risk of betrayal. This is known as the “assumption of risk” or “misplaced trust” doctrine, and it plays a large role in Fourth Amendment jurisprudence. It forms part of the Court’s reasoning in *Smith v. Maryland* and *United States v. Miller* (Chapter 8).

**Note 9 – Bugs, Transmitters, and Recording Devices**

*On Lee v. United States* holds that the Fourth Amendment does not apply when a concealed transmitter is placed on an informant. This case rests on the assumption of risk doctrine.

**LOPEZ V. UNITED STATES**

This is a case about bugging. The case turns on the assumption of risk doctrine. The Court concludes that this case follows from *On Lee*. The fact that electronic surveillance was used does not affect the Court’s analysis. Justice Brennan’s dissent argues that electronic surveillance makes a big difference. He accepts the assumption of risk doctrine but argues that electronic surveillance creates a different set of dangers. It is worth discussing the impact that electronic surveillance techniques have on existing doctrines.
Note 1 – Is Electronic Surveillance Different?

*Lopez* compares (1) electronic surveillance to (2) regular eavesdropping and decides that there is no “constitutional right to rely on possible flaws” in an agent’s memo. This note asks if these two activities should be considered as similar for constitutional purposes.

**KATZ v. UNITED STATES**

*Katz* is a central case, for it forms the foundation of modern Fourth Amendment jurisprudence. The Court overrules *Olmstead* and *Goldman*, and eliminates the notion of physical trespass. A key passage in the case states:

> 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 an area accessible to the public, may be constitutionally protected.

The import of this passage will be explored throughout the rest of Chapter 4. It might be worthwhile later on in the course to ask whether this passage still accurately reflects the state of Fourth Amendment law.

*Katz* establishes “the reasonable expectation of privacy” test, the Court’s current approach toward determining the applicability of the Fourth Amendment. The test is contained in a concurrence by Justice Harlan: (1) a person must exhibit an “actual (subjective) expectation of privacy”; and (2) “the expectation [must] be one that society is prepared to recognize as ‘reasonable.’”

Another aspect of the opinion worth discussing is the government’s argument that it had enough evidence here to establish probable cause. The government is, after all, operating under the *Olmstead* regime where it doesn’t need a warrant. And now, the Court has overturned *Olmstead*. The Court concludes that the warrant is not a mere formality. It might be worthwhile asking why. Warrants require judges to look prospectively, and judgments may differ when probable cause is evaluated in hindsight. The goal of the warrant requirement is to have judges involved before the search, not after the fact.

Note 1 – Who Was Charlie Katz?

David Sklansky provides interesting background about Katz and how the FBI recorded his calls.

Note 2—The Reasonable Expectation of Privacy Test

The Harlan concurrence in the *Katz* decision established the important test for assessing whether or not a reasonable expectation of privacy was present. Christopher Slobogin and Joseph Schumacher discuss how the Supreme Court has established “two significant guidelines” for interpreting what constitutes a reasonable expectation of privacy. First, the Court has indicated that defining a reasonable expectation of privacy should take into
consideration societal understandings. Second, the Court has sometimes used the word “legitimate” to describe expectations of privacy and has indicated that the Fourth Amendment does not protect expectations of privacy that only criminals would have.

Note 3 – Variations on *Katz*

*Katz* is in a glass phone booth on a public street, and the Supreme Court still concludes he has Fourth Amendment protection. This note poses some variations on the facts to help students focus on the key aspect in this case, that what the defendant “seeks to preserve as private” is constitutionally protected.

Note 4 – “Conditioned” Expectations of Privacy

This note quotes a footnote from *Smith v. Maryland* that asks what would happen if the government routinely engaged in totalitarian tactics, thus conditioning people to accept great invasions of privacy. Would people no longer have a reasonable expectation of privacy? The Court in the footnote says no – in these cases, people’s “expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was” and that a “normative inquiry would be proper.”

Note 5 – *Berger v. New York*

*Berger* is an important Fourth Amendment case decided by the Supreme Court before *Katz*. In *Berger*, the Court struck down parts of New York’s electronic surveillance statute as violating the Fourth Amendment. Among the flaws in the New York statute was its lack of particularity regarding a description of the specific crime that had been committed and the persons or things to be seized. It created a “blanket grant of permission to eavesdrop” that was “without judicial supervision or protective procedures.”

**UNITED STATES V. WHITE**

*United States v. White* involves an application of *Katz* to facts somewhat similar to those of *Lopez*. The difference here was that instead of a simple recording device, the conversations were transmitted simultaneously to the police over the radio. The case demonstrates how the Court’s pre-*Katz* doctrine of assumption of risk and the Court’s treatment of electronic surveillance devices fare under *Katz*. The Court first concludes that under the first prong of the reasonable expectation of privacy test, the defendant had a subjective expectation of privacy. On the second prong, however, the expectation is not reasonable. The Court concludes that this is an example of misplaced trust. This transmission is somewhat similar to a wiretap in that the police can listen in on the conversation as it is occurring. On the other hand, it differs because in the wiretap in *Katz*, none of the parties to the conversation were cooperating with the police.

Note 1 – *White* vs. *Katz*

This note asks whether the situation in *White* is more analogous to *Katz* rather than *On Lee* or *Lopez*. Why isn’t the simultaneous electronic eavesdropping in *White* akin to a wiretap?
White imports the “misplaced trust” doctrine from Hoffa and other cases into the post-Katz landscape of the Fourth Amendment.

**Note 2 – Covert Agents and the Misplaced Trust Doctrine**

In a comparative study, Jacqueline Ross discusses numerous differences in the regulation of undercover policing in the U.S. and Germany. The main difference is that German privacy law in this area seeks to protect dignitary interests while U.S. law emphasizes physical privacy in the home.

An interesting discussion can be had about whether covert agents and informants should be regulated by the Fourth Amendment. What if the misplaced trust doctrine were overturned? Law enforcement officials might be required to obtain a warrant before using a covert agent or informant. Is such an approach desirable?

**Note 3 – Electronic Surveillance and the First Amendment**

In dissent in White, Justice Douglas discusses the First Amendment protection of free discourse and how the monitoring of conversations threatens this constitutional value.

3. THE REASONABLE EXPECTATION OF PRIVACY TEST

The cases in this section focus on the application of the reasonable expectation of privacy test.

**(a) The Third Party Doctrine**

**Smith v. Maryland**

Smith v. Maryland is a key case. The Court holds that there is no reasonable expectation of privacy in the numbers a person dials that the police record with a pen register. The case turns on two rationales. First, the Court concludes that the numbers do not involve the “content” of the communications. This content vs. non-content distinction follows the division between the content of a letter and the envelope (or “mail cover”) and is also reflected in federal electronic surveillance law. Justice Stewart’s dissent questions this distinction, arguing that phone numbers reveal the identities of people with whom a person corresponds.

Second, the Court relies on the assumption of risk doctrine that when a person conveys information to another (the phone company), that person must assume the risk that the company will reveal the information to others. Justice Marshall’s dissent critiques this argument, contending that people do not have a choice whether or not the phone company has access to their dialed numbers.
CHAPTER 1. PRIVACY AND LAW ENFORCEMENT

Note 1 – Pen Registers and Trap and Trace Devices

This note emphasizes a key aspect of *Smith*: the content versus non-content distinction. Wiretaps record phone conversations – they collect the content of conversations. Telephone numbers, which were at stake in *Smith*, concern “telecommunication attributes,” or non-content aspects of the use of telephony.

Note 2 – Critiques of the *Smith* Decision

This note looks at some criticisms of *Smith*. For example, Patricia Bellia has noted that in *Katz*, the phone company also had a technical ability to hear the contents of the call. Yet, despite this technical ability, the Court found that Katz had a reasonable expectation of privacy in his conversation.

Note 3 – The Third Party Doctrine and Bank Records: *United States v. Miller*

This note focuses on two cases arising out of the passage of The Bank Secrecy Act of 1970, which required federally insured banks to retain records of the financial activities of their account holders and to report specified information about certain transactions. The Court struck down a challenge to the constitutionality of this Act in *California Bankers v. Shultz*. Though ultimately this challenge was resolved on standing grounds, Justice Douglas’s dissent echoes Justice Stewart’s discussion of the content vs. non-content distinction from *Smith v. Maryland*. Douglas emphasizes that financial records reveal substantial information about a person’s identity via their associations. Two years later, the Court in *United States v. Miller* relied on the third party doctrine in holding that an individual does not have a reasonable expectation of privacy in such records because they reflected information voluntarily turned over to banks.

Note 4 – The Scope of the Third Party Doctrine

This note questions where the line can and should be drawn regarding the scope of the third party doctrine. In particular, it raises this issue with respect to the sensitive area of medical records. Does the sensitivity of the information at hand play a role in this determination?

Note 5 – Federal and State Law

The *Smith* case was followed by Congress enacting the Pen Register Act. Its standards are significantly less stringent than those required to obtain a Fourth Amendment warrant.

Some statues have rejected *Smith* under their constitutions. For example, New Jersey found that there is a reasonable expectation of privacy in telephone records. It might be useful to point out to students that in a number of contexts, state constitutional law is more constraining than the Fourth Amendment. State constitutional constraints limit state police and officials, but they have no effect on what federal law enforcement officials may do.
Note 6 – Privacy of the Mail

Early Fourth Amendment case law prohibited the government from searching sealed letters without a warrant. Today, federal statutory law further limits the government’s ability to search the mail. The outside of letters and mail coming into the country from abroad, however, are not similarly protected.

Note 7 – Third Party Doctrine in the Information Age

In this note, Daniel Solove criticizes the continued application in the Information Age of the third party doctrine. When the third party doctrine was first established by Miller and Smith in the 1970s, the mass data storage practices of today did not yet exist. This note also asks about the consequences of overruling Miller and Smith?

Note 8 – Can a Contract or Promise Create a Reasonable Expectation of Privacy?

This note questions whether a written contract—by a company, for example, promising to keep its customers’ data confidential—should establish a reasonable expectation of privacy. Daniel Solove explains that contracts currently do not achieve this result, and challenges the fairness of this outcome in a society so heavily reliant on contract.

Note 9 – Critiques and Defenses of the Third Party Doctrine

This note collects a number of critiques of the third party doctrine. Susan Brenner and Leo Clark do not think that disclosure to a trusted party is the same as indiscriminate disclosure to the public. Daniel Solove notes that promises and contracts “are the foundation of modern civil society,” and the third party doctrine should not trump them. Thomas Crocker contrasts the Supreme Court’s protection of “conduct important to interpersonal relations” in Lawrence v. Texas with the third party doctrine, which leads to a view that “privacy protects only what we keep to ourselves.

In defense of the third party doctrine, Orin Kerr states that it protects “technological neutrality” in rules about the Fourth Amendment. Otherwise, criminals could use third parties “to create a bubble of Fourth Amendment protection” around criminal activity.

Note 10 – The First Amendment and the Third Party Doctrine

Daniel Solove views the First Amendment as a key and neglected source of constitutional criminal procedure rights. In his view, government access to pen register information can violate the First Amendment.

Neil Richards argues that the First Amendment protects a concept that he calls “intellectual privacy.” In so doing, the First Amendment safeguards the “ability . . . to develop ideas away from the unwanted gaze or interference of others.”
(b) Items Abandoned or Exposed to the Public

**CALIFORNIA V. GREENWOOD**

This case considers whether there is a reasonable expectation of privacy in the trash one leaves out at the curb. The assumption of risk doctrine applies in this case because trash is handed over to others (the garbage collectors). This case comes back into play when the Court considers the use of thermal imaging devices to detect the emanation of heat from the interior of a home in *Kyllo v. United States*.

**Note 1 – Recycling and Surveillance of Garbage**

In dissent in *Greenwood*, Justice Brennan views scrutiny of another’s trash as contrary to “notions of civilized behavior.” In the 21st century, the trend is for local communities to impose recycling obligations, which the sanitation department can oversee by spot checks on people’s trash. In such a community, one is on notice that there will be scrutiny of one’s trash. Does this scrutiny by the sanitation department affect whether an individual has a reasonable expectation of privacy in her garbage? If the sanitation department can check the trash to see if one has properly recycled, does it mean that the police department can check the trash as part of enforcing the criminal law?

**Note 2 – Surveillance 24/7**

Does the Fourth Amendment provide limitation on widespread, non-stop surveillance by the police? Presumably, it does not at present, if the surveillance is carried out from a publicly accessible vantage point. This note wonders whether there are nonetheless different normative issues raised by such police observation than a one-time search of any particular items, such as one’s luggage.

**Note 3 – State Courts and State Constitutions**

Some state courts have reached a different result than the Supreme Court in *Greenwood*. The note lists some of the analogies from an opinion of the Vermont Supreme Court, *State of Vermont v. Morris*, and asks if some are more convincing than the other.

**Note 4 – “Abandoned” DNA?**

The note describes the government’s increasing usage of DNA that has been “abandoned” in public for purposes of investigating crimes. An example on such abandoned DNA would be the DNA found on a discarded cigarette. Does *California v. Greenwood* preclude a reasonable expectation of privacy in genetic material that, like trash on the side of the curb, has been discarded?

One distinction may be that individuals do not expect that any third party, including the police, will collect their genetic material in this way. Elizabeth Joh argues that a warrant requirement should apply to collection of DNA for law enforcement purposes.
Another distinction concerns the fact that it is nearly impossible to avoid abandoning DNA, as DNA can be collected so readily from hair and saliva and other things. On the other hand, can people really avoid abandoning their trash?

One might argue that DNA involves more sensitive information than garbage. But this isn’t necessarily true in all cases. Garbage will invariably contain DNA information. And the items discarded can involve people’s personal papers, their medical supplies, and other things that will reveal very intimate details about their lives.

Maybe the Supreme Court just hadn’t realized the logical implications of *Greenwood* in an age where “abandoned” DNA can readily be analyzed.

On the other hand, suppose the police find a piece of clothing that looks like it has dried blood on it. Can they analyze the substance on the clothing to determine if it is blood? If the police find a book left in an alley, can they read it? Suppose it were written in French – can they translate it? If the answers are yes, then what is the difference when the police find DNA and analyze or “translate” it usable information?

**Note 5 – DNA by Deceit**

In *State v. Athan*, the police, posing as a law firm, sent a murder suspect a letter that requested a response by mail in order to receive compensation for settlement of a class action. The police used DNA from the suspect’s saliva on the returned envelope to connect him to a cold case. The Washington Supreme Court held that police have the ability to engage in “a limited amount of deceitful . . . conduct in order to detect and eliminate criminal activity.” It found that the government conduct at issue here was not so extreme as to coerce the defendant to commit a crime or disclose confidential information. As such, the defendant’s Fourth Amendment rights were not violated.

This case raises fascinating questions about the techniques the police used. Should the police be able to trick people into turning over information?

Police officers are permitted to go undercover and trick people into believing that they are trusted friends. Is the tactic used in *Athan* any more deceitful?

Suppose the police pretend to be doctors, nurses, or medical caregivers. They set up a fake doctor’s office. Is this kind of deceit appropriate? Or suppose a police officer pretends to be a religious leader and obtain a person’s confession? Or suppose a police officer pretends to be an attorney? Where is the line to be drawn?

**Note 6 – Who Decides What Constitutes a Reasonable Expectation of Privacy?**

This note examines the nature of the reasonable expectation of privacy test. Who should decide whether the test applies? Currently, the test is applied by the courts. But should it be? And if so, is the test empirical or normative? Courts often speak about societal views on privacy, yet they do so without citing to any authoritative sources. What should be used to measure society’s expectations of privacy? Polls?
Note 7 – Should the Reasonable Expectation of Privacy Test Be Empirical or Normative?

In this note, Daniel Solove argues that the law plays a profound role in shaping expectations of privacy. He points to the history of postal mail – people didn’t expect privacy in their letters, but the law responded to create protections. Indeed, perhaps one of the justifications for the legal protection of privacy is the fact that people desire privacy but don’t expect it. In other words, perhaps the reasonable expectation of privacy test shouldn’t look to what people currently expect to be private but to what people desire to be legally protected as private. Therefore, the test would measure society’s normative goals with regard to privacy. But the issues still remain – specifically, how should such normative preferences be measured?

Note 8 – Critiques of the Reasonable Expectation of Privacy Test

For Thomas Crocker, the Fourth Amendment protects “political liberty.” As a result, it should broadly protect “freedom of movement and social interaction in private and in public.”

Daniel Solove recommends that the Fourth Amendment “should provide protection whenever a problem of reasonable significance can be identified with a particular form of government information gathering.”

(c) Surveillance and the Use of Sense Enhancement Technologies

This section examines Fourth Amendment jurisprudence in the context of police surveillance and use of sense enhancement technologies, beginning with a brief background explanation of the plain view doctrine and the open fields doctrine.

Florida v. Riley

This case concludes that there is no reasonable expectation of privacy when the police flew in a helicopter 400 feet over the defendant’s greenhouse and observed marijuana plants through some translucent panels and missing panels in the roof. The case turns on the notion that this was a public vantage point; any member of the public could legally have been flying over the defendant’s property.

Note 1 – Privacy in Public

There are some instances in which one might have a privacy interest in a public setting. Katz states that the Fourth Amendment protects people, not places, yet it also states that what people expose to the public is not private. Does this mean that there is no reasonable expectation of privacy in a public place? One might argue that merely being in a public place does not extinguish one’s expectation of privacy. People conduct many activities in private in which they expect to be anonymous and not observed or scrutinized. But how should courts distinguish between when people are private in public and public in public?
Note 2 – Drones

The note explains the growing use of drones by law enforcement. The FAA has been given a key role for integrating so-called Unmanned Aircraft Vehicles into the nation’s airspace. How does Florida v. Riley shape Fourth Amendment protection in the context of drones? Will it make it more difficult to claim a reasonable expectation of privacy in regarding drones, or can it be distinguished?

Note 3 – Surveillance Cameras

This note considers the harms of surveillance cameras. Christopher Slobogin views the harm as changing how people act -- a surveillance camera is like having a police officer around twenty four hours a day, taking notes. This note also cites Jeffrey Rosen’s skepticism regarding the impact of surveillance cameras on violent crime in Britain.

Note 4 – Face Recognition Systems

The next step in surveillance cameras may be the use of face recognition systems. This note mentions trial runs of such a system in Tampa and at Super Bowl XXXV in January 2001. Phil Agre contends that face there is a “moral difference” between a single chance observation in a park and a camera system that observes individuals.

Note 5 – The First Amendment and Government Surveillance: Laird v. Tatum

This note explores the possibility that government surveillance might violate the First Amendment by chilling expressive, public conduct. While the Court in Laird v. Tatum held that mere allegations of “subjective” chilling did not constitute cognizable harm under the First Amendment, the Third Circuit in Philadelphia Yearly Meeting of the Religious Society of Friends v. Tate distinguished Laird and decided plaintiffs had established a chilling effect. The court emphasized that government surveillance of public activity was injurious in this case because information was disclosed to non-police agencies and the media. Would opening law enforcement surveillance to First Amendment challenges cast too far a net, given that all surveillance has the potential for inhibiting conduct?

DOW CHEMICAL CO. v. UNITED STATES

This case illustrates the effects of sensory enhancement technology. As in Florida v. Riley, it involves an aircraft fly-over. In contrast, however, here the EPA officials used a high-tech aerial camera, with magnification capabilities that could enlarge images in photographs. The Supreme Court concludes that the sense enhancement technology does not alter its analysis since the camera merely enhances what the naked eye could see. One aspect of the Court’s rationale is that the camera was available to the public. This point is of great importance, for it recurs in Kyllo v. United States.
Note 1 – New Surveillance Technologies

The public now has cheaper and more detailed satellite images available to it than ever before. Under the rationale of Dow Chemical, new technologies would be allowed to erode our reasonable expectation of privacy. On the other hand, if the law were not to change with new technologies, would it grow antiquated? In 1890, people might not have expected to have their photos taken in public. Today, the camera is in such widespread use that people are at least aware of the risk that somebody might take their photo.

Imagine a Fourth Amendment case involving the police using a camera back in the mid-nineteenth century that held that people had an expectation not to be photographed in public. Wouldn’t such a case rigidify the law, making it out-of-tune with modern times? In essence, it would be using the law to preserve basic societal values and expectations at a particular moment in time from changing. Is this a good or bad thing?

Note 2 – Flashlights

It is established in constitutional law that the use of flashlight to illuminate a darkened area does not constitute a search. The police need not use candles, nor obtain a search warrant before use of a flashlight. Can a distinction be made between a flashlight and other devices that enhance or extend the human ability to see, hear or smell?

Note 3 – Canine Sniffs

This note summarizes Fourth Amendment jurisprudence on law enforcement’s use of drug-sniffing dogs. United States v. Place holds that there is no reasonable expectation of privacy in a dog sniff of luggage. The Court concludes that the search is “less intrusive” than a physical search of the luggage because presumably only the possession of contraband will trigger a search. But it might be worthwhile asking whether the reasoning of this case brings back the Olmstead physical trespass notion. The Court takes care to try to keep the holding of the case very narrow because of the very “limited” nature of the search.

In Illinois v. Caballes, the Court found that conducting a dog sniff did not change the character of a traffic stop that was lawful at its inception and otherwise executed in a reasonable manner. Following the Court’s opinion in Place, the dog sniff was held to be sui generis because it detected only the presence or absence of narcotics. There was no legitimate expectation, according to the Court, in possessing contraband.

The Court clarified in Florida v. Harris that whether a narcotic dog’s alert provides sufficient probable cause depends on a totality of the circumstances test. A key factor under Harris is the dog’s reliability in a controlled setting.

Kyllo v. United States

Kyllo v. United States is the leading case on sensory enhancement technology. It involves the use of a thermal imager to detect heat patterns from the defendant’s home. The Court
concludes that the use of the device falls under the Fourth Amendment. The Court’s decision emphasizes the home as being at the core of Fourth Amendment protection as well that the lack of “general public use” of thermal imagers.

**Note 1 – Thermal Images vs. Cameras**

This note questions whether the distinction between the thermal imager at issue in *Kyllo* and the camera used in *Dow Chemical* is a valid one.

**Note 2 – Technology in General Public Use**

This note questions the Court’s use of whether a technology is in “general public use” to determine whether or not the Fourth Amendment will regulate it. Should the public’s access to a given technologic device matter at all for this constitutional assessment? IF thermal sensors are now more readily available, is *Kyllo* wrong due to changing facts?

**Note 3 – The Home**

The sanctity and privacy of the home has been recognized for centuries. This note explores various applications of this principle in American case law, from the extension of Fourth Amendment protection to apartment tenants in *Chapman v. United States* and later to overnight guests in another person’s home. Should a distinction be made between the police’s use of a thermal sensor directed at a home versus any other place, such as one’s office?

**Note 4 – The Courts vs. Congress**

This note revisits an issue that arises frequently in the course: which branch of government should make the rules? Orin Kerr argues that legislatures are better than courts in crafting rules to regulate new technologies.

**Note 5 – Is the Fourth Amendment Primarily Protective of the Individual or Society?**

Anthony Amsterdam asks whether the Fourth Amendment should be viewed as protecting individual citizens or a regulatory canon placed on the government to keep us collectively secure.

**Note 6 – Is Government Observation Different from Observation by Others?**

Amsterdam argues that observation by the police may violate privacy in the same way that the same observation by a neighbor or visitor may not.

**Note 7 – Beepers and Tracking Devices**

This note focuses on the use of beepers. *United States v. Knotts* holds that the Fourth Amendment does not apply to a beeper tracking the location of a car because there is no
reasonable expectation in one’s public movement. United States v. Karo, in contrast, holds that a beeper tracking the movements of a defendant within his home is a Fourth Amendment violation. The beeper cases are important as a set-up for Kyllo because the distinction between the two cases turns on the home.

United States v. Jones

In United States v. Jones, the Supreme Court held that law enforcement’s installation and use of a GPS tracking device on the undercarriage of a car constitutes a “search” within the meaning of the Fourth Amendment. The majority’s holding applied a common law property-based analysis that relied on the fact that police committed a physical trespass in installing the GPS device. The Court declined to decide whether or not such usage of GPS also violated defendant’s reasonable expectation of privacy. The Justice Scalia opinion emphasized that the Katz test supplemented but did not overrule a property-based approach to deciding the applicability of the Fourth Amendment.

In her concurring opinion, Justice Sotomayor agreed that the common law trespass test decided this case, but voiced concern about application of the reasonable expectation of privacy test to GPS monitoring. Extensive, aggregated government surveillance can reveal a significant amount of information about one’s identity and associations, a factor she cautions not to ignore in deciding whether there is a reasonable expectation of privacy in the “sum of one's public movements.”

Justice Alito concurred in the result, but argued against the majority’s application of a property-based analysis. He argued that long-term GPS surveillance violates one’s reasonable expectation of privacy and thus constitutes a “search.” He also argued that surveillance even in public can violate a reasonable expectation of privacy if the surveillance is very extensive. Neither Justice Alito nor Justice Sotomayor defined precisely where the line would be between ordinary surveillance and more pervasive surveillance.

Instructors might explore how police are to figure out when the Fourth Amendment would apply. There is no test, no clear place to draw the line. Students might be asked how they might define a test or a line. Other students can then critique the tests or lines that are proposed.

Note 1 – A New Direction?

Both concurring opinions argue that extensive and aggregated surveillance of public movements can impinge on an individual’s reasonable expectation of privacy if done for a long enough period. Does this acknowledgement of legitimate privacy concerns surrounding conduct that occurs in public represent a new direction for the Katz test?

Note 2 – Influence on Other Areas of Privacy Law

Would the concurring opinions’ argument for Fourth Amendment protection against extensive surveillance of public movements affect the privacy torts? This note references
the concept in *Nader v. GM* (Chapter 3) concerning “overzealous” surveillance in public as a violation of privacy.

**Note 3 – Where is the Line?**

This note considers the views of different scholars concerning the “mosaic theory.” Both Daniel Solove and Helen Nissenbaum have supported the idea that the aggregation of isolated pieces of information can constitute a profound violation of privacy. In contrast, Orin Kerr has rejected this approach.

**Note 4 – Dogs, the Home, and Property-Based Protection of Privacy**

This note discusses *Florida v. Jardines*, which ties together *Kyllo*’s emphasis on protection for the home with *Jones*’s emphasis on a trespass-based approach to applying the Fourth Amendment. In this case, the police conducted a dog sniff on the porch of defendant’s home. Justice Scalia wrote for the majority, holding that the front porch falls within the curtilage of the home and thus garners strong Fourth Amendment protection. Justice Kagan wrote a concurring opinion that likened the use of a narcotics dog to detect contraband in the home’s interior to the use of the thermal imager in *Kyllo*. Justice Alito in dissent argued against such a comparison since drug-sniffing dogs were not a new form of technology, unlike the thermal imager, and have been used for centuries without any common law judge finding that their use represented a trespass. Alito also argued against a dog sniff offending a property-based analysis of the Fourth Amendment given the brief, limited nature of the police’s approach of the home.

**B. INFORMATION GATHERING ABOUT FIRST AMENDMENT ACTIVITIES**

This section examines the intersection between the Fourth and the First Amendments, focusing on government surveillance that implicates the various freedoms protected by the First Amendment.

**Stanford v. Texas**

In *Stanford v. Texas*, police seized a significant amount of miscellaneous books and documents from petitioner’s home pursuant to a warrant, which was issued due to his suspected involvement in the Communist Party of Texas. A unanimous Supreme Court held that the search violated petitioner’s Fourth Amendment rights because the warrant at issue was too broad in scope, which made it an unconstitutional general warrant. The Court established that the particularity and probable cause requirements for warrants must “be accorded the most scrupulous exactitude” when the materials sought to be seized implicate the First Amendment.
Note 1 – Are Fourth Amendment Warrants Sufficient to Protect First Amendment Activities?

The Court later clarified in *Zurcher v. The Stanford Daily* that while the Fourth Amendment requires “scrupulous exactitude” when First Amendment protections are implicated, probable cause suffices to render a warrant constitutional under the Fourth Amendment. This and later cases stand for the proposition that *Stanford v. Texas* does not require a heightened constitutional standard for seizing materials, like books, that are protected by the First Amendment. Rather it requires “particular exactitude when First Amendment interests would be endangered by the search.”

Note 2 – The Privacy Protection Act

This note briefly describes the Privacy Protection Act, which was passed as a response to *Zurcher* to protect the freedom of the press under the First Amendment.

Note 3 – Government Information Gathering About Group Membership

This note compares a handful of cases concerning government investigations that implicate the freedom of association protected by the First Amendment. Two of the cases involved state bar associations asking about membership in the Communist Party. Do the associations of attorneys raise distinct issues?

Note 4 – Intellectual Privacy

Neil Richards argues that the First Amendment protects a concept that he calls “intellectual privacy,” meaning the ability to safely generate and test new ideas without “unwanted interference.” He views belief formation as falling within the First Amendment’s scope given the importance of developing ideas, even controversial ones, to the practice of truly free speech. Would Richards’ argument unduly extend the protections of the First Amendment?

Note 5 – The First Amendment as Criminal Procedure

This note explores Daniel Solove’s argument that the First Amendment can and should be invoked in cases of government searches and surveillance that trigger its protections. In his view, it would operate somewhat similarly to the Fourth Amendment. Should it? What kinds of government information gathering would trigger its application?

**GONZALEZ v. GOOGLE**

In *Gonzalez v. Google*, the Department of Justice subpoenaed from Google a random sample of URLs and 5,000 search queries, but not any additional information identifying the Google users who entered the search terms. The court upheld the subpoena as to the URL sample, but quashed the government’s subpoena for Google users’ search terms. Google challenged the search query subpoena on the grounds that Google would be
“unduly burdened by [the] loss of user trust” that would result from failing to protect its users’ privacy.

**Note 1 – URL Samples vs. Search Queries**

Why does the court reach different results for the two kinds of data subpoenaed in *Gonzalez v. Google*?

**Note 2 – Can People Be Identified from Anonymous Search Data?**

AOL demonstrated that people can in fact be identified from their search queries, even when the queries were disassociated from usernames and assigned anonymous numerical IDs. What are the implications of this finding?

**C. FEDERAL ELECTRONIC SURVEILLANCE LAW**

**1. SECTION 605 OF THE FEDERAL COMMUNICATIONS ACT**

This section provides a brief discussion of § 605 of the Federal Communications Act of 1934, the early precursor to modern federal wiretap law. It might be worthwhile to point out that § 605 is an example of the recurrent theme of the judiciary versus the legislature. In *Olmstead*, the Court interpreted the Constitution narrowly, prompting Congress to respond by regulating wiretapping by statute.

Another interesting issue raised by § 605 concerns the problem with trying to prohibit electronic surveillance as opposed to regulating it. Section 605 prevented the government from gathering evidence for a trial by means of wiretapping, but the government was otherwise free to wiretap. Many abuses followed. Compare this approach with the more elaborate regulatory structure enacted by the Congress in 1968. The problem arises also in other countries where constitutional provisions appear to prohibit electronic surveillance.

**2. TITLE III**

This section discusses Title III, which has become the foundation of modern federal wiretap law. Again, it might be worthwhile to point out that Title III was passed just a year after *Katz v. United States*. In contrast to the passage of § 605, which filled the void when the *Olmstead* Court declared that the Fourth Amendment does not apply to wiretapping, Title III supplements *Katz*.

**3. ELECTRONIC COMMUNICATIONS PRIVACY ACT**

This section discusses the Electronic Communications Privacy Act (ECPA), which forms the basis of modern federal wiretap law.

It might be useful to point out that the ECPA restructures Title III. The old Title III now comprises the Wiretap Act, sometimes referred to as “Title I” of ECPA. The Stored
Communications Act (Title II of ECPA) adds protections for stored communications. The Pen Register Act (Title III of ECPA) concerns pen registers and trap and trace devices.

ECPA is a very complicated statute. This section attempts to explain ECPA in a clear and accessible manner. The reading can be somewhat dry, but it is helpful to explain some of the basics to the students.

Some key points to cover:

1. A key to understanding ECPA is to understand the three types of communications it covers. These are defined in the Wiretap Act, but the terms are also used in the Stored Communications Act (SCA). The ECPA covers three types of communications:

   (1) **Wire Communications**: A “wire communication” involves “aural transfers” (communications containing the human voice) that travel in part or whole through wire (i.e. telephone wires or cable wires) or a similar medium. See 18 U.S.C. § 2510(1).

   (2) **Oral Communications**: An “oral communication” is a communication “uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.” Such communications are typically intercepted through bugs or other recording or transmitting devices. See 18 U.S.C. § 2510(2).

   (3) **Electronic Communications**: An “electronic communication” consists of all non-wire and non-oral communications (i.e. signals, images, data) that can be transmitted through a wide range of transmission mediums (wire, as well as radio, electromagnetic, photoelectronic, etc.). An email is an example of an electronic communication. See 18 U.S.C. § 2510(12).

The type of communication at issue is important under ECPA, because different types of communications receive different levels of protection. For example, wire and oral communications are protected by the exclusionary rule under the Wiretap Act, but electronic communications are never protected by the exclusionary rule.

2. The Wiretap Act provides significantly more protection than the SCA. The Wiretap Act has an exclusionary rule, greater civil and criminal penalties, and stricter requirements for court orders. A court order under §2518 provides more protection than an ordinary warrant, and it is sometimes referred to as a “super warrant.” There is, however, one dimension in which this court order is less protective than a warrant. In contrast to warrants, which are generally short in duration, the §2518 order can last up to 30 days.

3. The Stored Communications Act (SCA) covers communications in “electronic storage,” a term defined in the definitions section of the Wiretap Act. See §2510(17). It is easy to assume that SCA applies broadly to stored communications, but looking at the plain text of the definition complicates matters. The definition defines storage as “any temporary, intermediate storage” that is “incidental” to the communication and “any storage of such
communication by an electronic communications service for purpose of backup protection of such communication.” The statute says “and,” but this seems extremely limiting, and courts often read these two prongs of the definition separately. Additionally, must storage be temporary and incidental? This is also quite limiting.

4. The SCA also covers records held by ISPs. These records contain information about subscribers and are important because they can link a person’s online pseudonym to her identity.

5. The Pen Register Act provides limited protection of pen registers and trap and trace devices, which the Court held fell outside the Fourth Amendment in *Smith v. Maryland*. The court order under the Pen Register Act does not require probable cause. Judges have little discretion in refusing to grant pen register orders. If the government certifies that the “information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation,” then the judge “shall” grant the order.

The following chart may be of help. It is included on a separate page if instructors desire to provide it as a handout.
### THE ELECTRONIC COMMUNICATIONS PRIVACY ACT IN A NUTSHELL

**By**

Daniel J. Solove & Paul M. Schwartz

_for use in conjunction with_ 


<table>
<thead>
<tr>
<th>Codified</th>
<th>THE WIRETAP ACT</th>
<th>THE STORED COMMUNICATIONS ACT</th>
<th>THE PEN REGISTER ACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Provisions</td>
<td>Interception of communications in flight</td>
<td>(1) Accessing communications in “electronic storage”; (2) Records of ISPs</td>
<td>Pen registers and trap and trace devices</td>
</tr>
<tr>
<td></td>
<td><strong>Interception</strong>: provides strict controls on the “interception” of communications. “Interception” is the acquiring of the contents of a communication through an electronic, mechanical, or other device while the communication is being transmitted.</td>
<td><strong>Stored Communications</strong>: requires the government to obtain via court order, subpoena, or warrant. § 2703</td>
<td>Requires court order before installation of pen registers and trap and trace devices.</td>
</tr>
<tr>
<td>Exceptions</td>
<td>Consent: Wiretap Act does not apply if one party to the communication consents. §2511(2)(c).</td>
<td>Consent: SCA does not apply if the subscriber consents. §2702(b).</td>
<td>Service Provider: SCA does not apply to the accessing of stored communications by communications service providers. §2701(c)(1).</td>
</tr>
<tr>
<td></td>
<td><strong>Service Provider</strong>: Wiretap Act does not apply to the interception of communications by a communications service provider. §2511(2)(a)(i).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>THE WIRETAP ACT</td>
<td>THE STORED COMMUNICATIONS ACT</td>
<td>THE PEN REGISTER ACT</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Court Order</td>
<td>Application for court order to intercept must contain details justifying the interception and information about how the interception will occur and its duration. §2518</td>
<td>Communications Stored 180 Days or Less: Government must obtain warrant supported by probable cause. §2703(a)</td>
<td>The government must obtain a court order to install pen register and trap and trace devices.</td>
</tr>
<tr>
<td></td>
<td>The judge must find: (1) probable cause (2) alternatives to interception had failed, are unlikely to succeed, or will be too dangerous. Orders must require that interception be conducted to “minimize the interception of the communications not otherwise subject to interception.” §2518(6).</td>
<td>Communications Stored 180 Days+: Government must provide prior notice to subscriber and obtain a subpoena or court order. §2703(b)</td>
<td>The court “shall” grant the order if the government has demonstrated that “the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.” §3123(a).</td>
</tr>
<tr>
<td></td>
<td>Only high level government prosecutors can apply for orders. Orders are limited to certain crimes (most felonies); orders cannot be obtained to investigate misdemeanors.</td>
<td>Court order requires “specific and articulable facts showing that there are reasonable grounds” to believe communications are relevant to the criminal investigation. §2703(d)</td>
<td></td>
</tr>
<tr>
<td>Exclusionary Rule</td>
<td>Yes, for wire and oral communications. No, for electronic communications</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Penalties</td>
<td>Damages (minimum $10,000 per violation) §2520</td>
<td>Damages (minimum $1,000 per violation) §2701(b)</td>
<td>Fines. Up to 1 year imprisonment §3123(d).</td>
</tr>
<tr>
<td></td>
<td>Up to 5 years imprisonment. §2511</td>
<td>Up to 1 year imprisonment (if done for commercial gain) §2701(b)</td>
<td></td>
</tr>
</tbody>
</table>
# THE FOURTH AMENDMENT vs. FEDERAL ELECTRONIC SURVEILLANCE LAW

<table>
<thead>
<tr>
<th>Applicability</th>
<th><strong>FOURTH AMENDMENT</strong></th>
<th><strong>FEDERAL ELECTRONIC SURVEILLANCE LAW</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Fourth Amendment applies to electronic surveillance when there is a reasonable expectation of privacy. The Fourth Amendment applies only to government officials (subject to limited exceptions).</td>
<td>Federal electronic surveillance law applies to all interceptions of communications and to accessing stored communications (even if there is no reasonable expectation of privacy). Federal electronic surveillance law applies to pen registers and trap and trace devices (Pen Register Act). The Fourth Amendment does not apply to these devices. <em>See Smith v. Maryland.</em> Federal electronic surveillance law applies to government officials and to private parties.</td>
</tr>
</tbody>
</table>

| Judicial Authority to Obtain Access | Subject to a number of exceptions, the Fourth Amendment requires a warrant supported by probable cause. | Federal electronic surveillance law contains a wide variety of forms of judicial authority, including subpoenas, court orders with varying levels of notice to the subject of the investigation, warrants, and the super warrant required by the Wiretap Act. |

| Duration of Authority to Obtain Access | Fourth Amendment warrants authorize a single entry and prompt search. Warrants must be narrowly circumscribed. The Fourth Amendment is enforced by the exclusionary rule. The Fourth Amendment can serve as the basis for a §1983 or *Bivens* action. | Federal wiretap orders have a rather broad duration. A judge can authorize 24-hour surveillance for a 30-day period. Federal electronic surveillance law is enforced through the exclusionary rule only sometimes – for interceptions of wire or oral communications under the Wiretap Act. Federal electronic surveillance law also has civil and criminal penalties. |

<table>
<thead>
<tr>
<th>Enforcement</th>
<th><strong>FOURTH AMENDMENT</strong></th>
<th><strong>FEDERAL ELECTRONIC SURVEILLANCE LAW</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Applicability**

The Fourth Amendment applies to electronic surveillance when there is a reasonable expectation of privacy. The Fourth Amendment applies only to government officials (subject to limited exceptions).

**Federal Electronic Surveillance Law**

Federal electronic surveillance law applies to all interceptions of communications and to accessing stored communications (even if there is no reasonable expectation of privacy). Federal electronic surveillance law applies to pen registers and trap and trace devices (Pen Register Act). The Fourth Amendment does not apply to these devices. *See Smith v. Maryland.*

Federal electronic surveillance law applies to government officials and to private parties.

**Judicial Authority to Obtain Access**

Subject to a number of exceptions, the Fourth Amendment requires a warrant supported by probable cause.

**Federal Electronic Surveillance Law**

Federal electronic surveillance law contains a wide variety of forms of judicial authority, including subpoenas, court orders with varying levels of notice to the subject of the investigation, warrants, and the super warrant required by the Wiretap Act.

**Duration of Authority to Obtain Access**

Fourth Amendment warrants authorize a single entry and prompt search. Warrants must be narrowly circumscribed. The Fourth Amendment is enforced by the exclusionary rule. The Fourth Amendment can serve as the basis for a §1983 or *Bivens* action.

**Federal Electronic Surveillance Law**

Federal wiretap orders have a rather broad duration. A judge can authorize 24-hour surveillance for a 30-day period.

**Enforcement**

Federal electronic surveillance law is enforced through the exclusionary rule only sometimes – for interceptions of wire or oral communications under the Wiretap Act. Federal electronic surveillance law also has civil and criminal penalties.
4. THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

This section provides a brief introduction to the Communications Assistance for Law Enforcement Act (CALEA). Broadly speaking, the CALEA requires telecommunications companies to build in surveillance capabilities for law enforcement into new technologies. Instructors may want to have students discuss whether, as a policy matter, the developers and providers of technology should be required to do this.

5. THE USA-PATRIOT ACT

The USA PATRIOT Act is covered separately because it is best studied after the students have an extensive background into federal electronic surveillance law.

This section describes some of the many changes the USA PATRIOT ACT made to electronic surveillance law.

6. STATE ELECTRONIC SURVEILLANCE LAW

This section provides a brief discussion of state electronic surveillance law. Many state laws are similar to ECPA, though a minority of states have laws that diverge in one key respect – they require all parties to consent, not just one. These statutes are known as “all party consent laws.”

D. DIGITAL SEARCHES AND SEIZURES

Whereas Part C above is mostly expository, introducing the basic concepts and framework for electronic surveillance law, this Part explores how electronic surveillance law and the Fourth Amendment apply to various searches and seizures involving digital information.

1. SEARCHING COMPUTERS AND ELECTRONIC DEVICES

This section examines searches of computers and electronic devices. 

*United States v. Lacy* involves the issue of the scope of warrants for the searching and seizure of computers. The court concludes that a warrant authorizing a seizure of the defendant’s computer was not too broad because greater precision in the warrant wasn’t possible.

A case subsequent to *Lacy*, *U.S. v. Campos*, found that the FBI was not required to search only for particular computer files in one’s home. The controlled environment of a laboratory was essential to complete analysis of the files.

In *Trulock v. Freeh*, the court looked at a situation in which two people shared a computer, but maintained separate files protected by passwords. They did not know each other’s passwords and could not access each other’s files. The court found that one user could
consent to a general search of the computer, but not to the other user’s password-protected files.

**United States v. Andrus**

This case considers the conditions under which valid third party consent can arise to a police search. The consent can be valid either when the third party has actual authority or merely apparent authority. The test for valid apparent authority is an objective one—would a reasonable officer believe the third party had authority to consent to the search. Under the facts of this case, the court decided that it was reasonable for the police officers to believe that the parent had authority to consent to the search.

The dissenting judge argued that in consent-based, warrantless computer searches, law enforcement personnel were required to inquire or otherwise check for the presence of password protection and, should a password be present, ask the consenter about his knowledge of that password and joint access to the computer.

**Note 1 – A Question of Perspective?**

Orin Kerr argues that the case looks quite different depending upon whether one views it from a virtual or physical perspective.

**Note 2 – Checking for Password Protection**

This note asks whether this decision creates an incentive for the police to ask as few questions as possible to a consenter to a computer search. The ideal is to gain just enough information so that the consent to the search can be seen as objectively reasonable.

**Note 3 – The Right to Delete**

Paul Ohm argues that the Fourth Amendment extends to a “right to destroy,” or delete, data that the government has seized. This interest goes beyond a right to merely exclude it from use at a trial.

**Note 4 – Computer Searches at the Border—and Beyond**

The Supreme Court grants broad powers for the government to engage searches at the border. A range of issues occur when computers and other electronic devices are examined at the border. In *United States v. Cotterman*, the Ninth Circuit upheld a search of a laptop computer that began at a border and then continued for two days in a government forensic laboratory that was 170 miles away. For the Ninth Circuit, one of the key factors in its decision was that the defendant never regained a normal expectation of privacy in his computer.
Note 5 – Government Access to Data Stored in Other Countries

This note discusses *Microsoft Corp. v. United States (Microsoft Ireland)*. The court held that the government could not use of a warrant under the Stored Communications Act for data located outside the United States.

**RILEY v. CALIFORNIA**

*Riley v. California* concerns two cases in which police seized cell phones from arrestees and searched the digital information contained on the devices without first obtaining a warrant. The Supreme Court held that such a search was unreasonable and thus in violation of the Fourth Amendment. The quantitative and qualitative differences between the data stored on a cell phone and the physical effects capable of being seized from an arrestee’s person factored heavily into the Court’s reasoning; cell phones, capable of storing massive amounts of information, hold the “privacies of life” for most people. The Court sharply distinguishing the contents of cell phones from other physical items traditionally subject to warrantless search incident to arrest.

Note 1 – A Quantitative Difference?

This note points out that in both *Riley v. California* and *Jones*, the Supreme Court focused on the enormous quantity of information stored, respectively, on cell phones and via GPS devices. This note questions whether the Court has clarified a test that distinguishes searches of these devices from other searches.

Note 2 – Implications for *Smith v. Maryland*

In *Riley*, the Supreme Court rejected the argument that the third party doctrine should allow law enforcement to search a cell phone’s call log without a warrant because cell phone user’s often add identifying information to the stored numbers. Does this holding overturn *Smith v. Maryland*, which found no expectation of privacy in the numbers one calls?

Note 3 – Implications for the Third Party Doctrine

Daniel Solove suggests that *Riley* may demonstrate a Court less willing to rely on the third party doctrine in the Information Age. Solove argues that the type of data and the information at issue should instead decide the question of whether a reasonable expectation of privacy exists. Can *Riley* be reconciled with the third party doctrine, or is the Court recognizing its unsuitability to modern technology?

2. ENCRYPTION

*Junger v. Daley* concluded that the First Amendment extended its safeguards to encryption as protected speech. A different result was reached by the D.C. Circuit in 1996 in *Karn v. U.S. Dep’t of State*. The Karn court found the contested regulation of encryption to be content neutral and justified under the applicable First Amendment test.
3. **VIDEO SURVEILLANCE**

Silent visual surveillance is not covered under federal electronic surveillance law. Because there is no interception or “oral” communication involved, the Wiretap Act does not apply, and because there is no accessing of stored images, the SCA does not apply. The requirements of the Fourth Amendment, however, do generally apply to government use of video surveillance.

4. **EMAIL**

**STEVE JACKSON GAMES v. UNITED STATES SECRET SERVICE**

This case applies ECPA to the seizure of a computer containing the unread email of private parties. Does the seizure of the email constitute an interception under the Wiretap Act? The argument for why the emails may still be in flight is that they haven’t yet reached their final destination. Suppose X sends an email to Y. X’s email goes to Y’s ISP and stays there until Y logs on and downloads her email. Once the email is downloaded, Y has received it. Analogized to sending a letter through the mail, the letter hasn’t reached its final destination until it is delivered to the addressee. However, the court holds that under ECPA, the email is *not* in flight. In flight means in transmission, and the email sitting on the ISP’s computer is at best a stored communication, subject to the SCA’s lesser protections.

**Note 1 – Interception vs. Electronic Storage**

The email on the ISP’s server is in storage because it is sitting on a hard drive rather than being “in flight” on the way to the recipient. One might view it as still “on its way” to the addressee until it arrives at her computer, but the *Steve Jackson Games* court did not interpret ECPA in this fashion.

**Note 2 – The Fourth Amendment and E-mail: A Question of Perspective?**

This note discusses *Orin Kerr’s* idea that we sometimes view the Internet from an “internal” perspective, and sometimes from an “external” perspective. These different perspectives will affect the answer regarding whether the Fourth Amendment requires a search warrant before law enforcement officers can obtain emails from an ISP.

**Note 3 – Previously Read E-mail Stored at an ISP**

This note examines the issue of how previously read email fits into the SCA. Today, because of the large amount of storage space available, people often keep their previously read emails without deleting them. The SCA appears to have been written to address stored email before it has been read. The note explores the issue and how courts are attempting to resolve it.
Note 4 – What Constitutes an Interception?

This note looks at the controversial decision in *United States v. Councilman*. A panel for the 1st Circuit interpreted the Wiretap Act extremely narrowly, thus significantly limiting the definition of “interception.” The case generated a significant public outcry, and the 1st Circuit reheard the case en banc and reversed. The en banc court concluded that the term “electronic communication” includes transient electronic storage that is intrinsic to the communication process for such communications. An email message does not, therefore, cease to be an “electronic communication” during the momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage.

Note 5 – Carnivore

Carnivore presents some interesting issues about the applicability of the Fourth Amendment in the context of the Carnivore. This issue was not resolved by any court. Moreover, as the casebook notes, the FBI discontinued use of the Carnivore device in 2005 because ISPs can now readily produce the information that the FBI desires without use of this device. Commercially available software allows the FBI to reach this functionality without use of the Carnivore device.

**United States v. Warshak**

In *Warshak*, the Sixth Circuit found that Warshak had a subjective expectation of privacy in his e-mails and that this expectation was also objectively reasonable, and, therefore, protected by the Fourth Amendment. The government had seized about 27,000 of his e-mails from Warshak’s ISP. The Sixth Circuit drew analogies with the protection granted to letters and rented space, and noted the inevitability of recourse to an ISP if one wished to send e-mails. At the same time, however, the court cautioned that a subscriber agreement might be broad enough to defeat a reasonable expectation of privacy. It also distinguished the Supreme Court’s decision in *United States v. Miller*. Finally, the Sixth Circuit found that government relied in good faith on the SCA and, therefore, the emails were not subject to the exclusionary remedy.

Note 1 – Email and the Third Party Doctrine

This note asks whether the Sixth Circuit convincingly distinguished its holding from the Supreme Court’s third party doctrine cases, such as *United States v. Miller*. In that case, it held of a bank customer:

> The depositor takes the risk in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed to him to Government authorities, even if the information is revealed on the assumption that it will be used for a limited purpose and the confidence placed in the third party will not be betrayed.
The *Warshak* court stated that (1) *Miller* involved simple business records, where emails represented a different category due to the “potentially unlimited variety” of communications involved; and (2) a bank depositor turned information over to the bank for its use in business, but an ISP was only an intermediary.

**Note 2 – The SCA and Email**

*Patricia Bellia* and *Susan Freiwald* argue that warrant-level protection for stored e-mail should continue, and not turn on whether the email in question has been “opened, accessed, or downloaded.”

**Note 3 – Keystroke Logging Systems**

*United States v. Scarfo* involves the use of a device known as a Key Logger System, which recorded the defendant’s keystrokes on his computer to figure out his password. Scarfo argues that the government’s use of the keystroke logger violated ECPA. The court analyzes whether the Wiretap Act applies; the key issue was whether there is an “interception” of a communication. For there to be an interception, the communication must be in transit. Here, according to the court, there was no interception because the key logger didn’t record keystrokes while Scarfo’s modem was operating. In other words, recording keystrokes prior to transmission over a wire is not an interception.

Suppose a person types a letter and then emails it to another computer. If the FBI captures the person’s keystrokes before the letter is sent, there is no interception. If the FBI taps the line and intercepts the email as it is traveling through the line to the other computer, then there is an interception. It might be useful to recall the narrow interpretation of interception in *Steve Jackson Games*. How narrowly or broadly should ECPA be interpreted?

Much of the discussion in *Scarfo* is moot, however, since there is no suppression remedy under the Wiretap Act available for the plaintiff.

*Raymond Ku* argues that the recording of keystrokes permits the government “to monitor thought itself.” Instructors might ask whether this analogy holds up. What kinds of activities, while not directly indicative of thought, are nevertheless close enough to it to warrant protection? Writing? Reading? Web-surfing? Speaking?

**5. ISP ACCOUNT INFORMATION**

**United States v. Hambrick**

This case stems from the police using a clearly invalid subpoena to obtain ISP records about a pseudonymous individual. The defendant makes an intriguing argument, which the court ultimately rejects. To understand why the defendant makes the argument he does, it is important to analyze the case under both the Fourth Amendment and federal electronic surveillance law (ECPA). Under the Fourth Amendment, *Smith v. Maryland* would suggest that there is no reasonable expectation in ISP records because they are maintained by a third party (assumption of risk doctrine). Under ECPA, the SCA requires a valid
warrant in order for ISPs to disclose their records to the government. At first glance, it appears the SCA might have been violated. More on this issue later.

Even if violated, ECPA would not be helpful to Hambrick in his criminal case because there is no exclusionary rule under the SCA. So Hambrick comes up with an interesting and creative argument. He argues that under the Fourth Amendment there is a reasonable expectation of privacy in his ISP records because the ECPA “legislatively resolves” this question. Although Smith suggests there is no reasonable expectation of privacy here, Congress enacted the ECPA in 1986 providing protection. The fact that Congress protected ISP records is evidence that society recognizes an expectation of privacy in these records. The Hambrick court, however, rejects this argument, concluding that ECPA doesn’t legislatively resolve this question because there is no suppression remedy for SCA violations and ECPA does not prohibit ISPs from disclosing their records to private parties.

One could further argue that there is no ECPA violation here either, despite the fact that the subpoena was clearly invalid. The language of the SCA focuses on prohibiting ISPs from disclosing records to the government and does not speak to the actions of the government. On the ISP’s end, it followed what it thought in good faith to be a valid arrant. Thus, ECPA provides no remedy. The provision doesn’t apply to the government and the ISP has a good faith defense. The impropriety of the government’s actions falls outside of ECPA. This result will strike many as unfair and contrary to common sense. Indeed, the court in McVeigh v. Cohen articulates a different view of this provision of the ECPA, namely, that it imposes a reciprocal obligation on the part of the government.

One important fact to note about Hambrick is that the disclosure of ISP records was used to reveal the identity of a pseudonymous individual. As will be explored in Chapter 3, the First Amendment also protects anonymous communication. Should the First Amendment apply whenever the government seeks to obtain records that would identify an anonymous or pseudonymous speaker? Would the First Amendment impose any additional requirements before the government can obtain ISP records beyond those specified in the SCA?

**Note 1 – Is There a Reasonable Expectation of Privacy in ISP Records?**

The district court in *U.S. v. Kennedy* reached a similar conclusion to the court in *Hambrick*. The *Kennedy* court relied as well on *Smith v. Maryland*.

**Note 2 – Statutes as a Basis for a Reasonable Expectation of Privacy?**

Where does a reasonable expectation of privacy come from? Purportedly, it arises because out of a societal recognition of privacy. This note discusses the consequences and implications of resting a societal recognition of a reasonable expectation of privacy on a statute that protects information privacy. On the one hand, statutes are a major source of societal views, since this is what members of a democratic society have chosen to enact via their elected representatives. Statutes might therefore be the prime source for recognizing a reasonable expectation of privacy.
On the other hand, if courts use statutes protecting privacy to recognize a reasonable expectation of privacy under the Fourth Amendment, then this might prevent legislatures from enacting privacy-protective laws if they do not desire to bring something within the governance of the Fourth Amendment. Would Congress have passed the SCA if it meant an exclusionary rule would be applied? If the defendant’s argument is to be accepted, then Congress might not pass laws like the SCA because of the fear that such laws would lead to courts applying the Fourth Amendment and the exclusionary rule.

Note 3 – Is There a Remedy?

This note examines remedies for government violation of the SCA. Mindspring escapes liability because it released information in response to a governmental subpoena (albeit an invalid one). If there is no remedy against the police in this case then, there is a loophole in the law that allows officers to falsify subpoena without consequences.

*McVeigh v. Cohen* involves the Navy’s attempt to discover the identity of a person using AOL screen name “boysrch.” A Navy official calls AOL and states that he received a fax to boysrch and wanted to confirm who it belonged to. The AOL representative identified the person as Timothy McVeigh (no relation to the Oklahoma City bomber). The Navy then sought to discharge McVeigh under the “Don’t Ask, Don’t Tell, Don’t Pursue” policy. The court’s decision hinges largely on the nature of the “Don’t Ask, Don’t Tell” policy, concluding that the Navy impermissibly “asked” and “pursued” under the policy.

The court also discusses the ISP records provision of the ECPA. The Navy contends that §2703(c)(1)(B) places the obligation on the ISP to withhold information from the government. AOL might have violated this provision, but not the Navy. The court, however, concludes that the government has a reciprocal obligation to follow this provision. This seems to follow common sense. If the government didn’t have an obligation, then it could use trickery and deceit to induce an ISP to violate the provision, as it did here by posing as a private party.

The court states that “it is elementary that information obtained improperly can be suppressed where an individual’s rights have been violated,” suggesting that there might be a judicially imposed exclusionary rule to this provision of ECPA. The SCA, however, has no exclusionary remedy. This note asks for a discussion about whether it is appropriate for courts to create one.

Subsequent to *McVeigh*, Congress amended ECPA to make clear that the relevant provisions applied not only to ISPs but also to the government, but did not add an exclusionary rule.

Note 4 – Cell Site Location Information

Beyond the use by the government of a GPS device to track a person in public, the government can gain information about a person’s movement or location by gaining access to data about a person’s cell phone from her telecommunications service provider. This note discusses two cases that have attempted to derive the correct standard for the
government before it can obtain such information. Is cell-site locational information analogous to GPS tracking? The information gleaned about a person may be similar, but GPS tracking occurs in real-time and cell-site locational information often involves information about past movement. Instructors may want to discuss with students whether there should be a difference in how the law treats information obtained in real-time vs. historically.

Note 5 -- Historical vs. Real-Time Location Data

Some courts have made a distinction between historical and real-time locational data. Only the latter are sometimes found to require a warrant. Susan Freiwald has rejected this distinction; in her view, both kinds of data are similarly informative for law enforcement officials and represent the same kind of burden on privacy. An instructor might simply ask how the class views the privacy implications of collection of information about their location for the five hours after class on one day last month versus the same kind of data captured by the government in real time today.

6. IP ADDRESSES, URLs, AND INTERNET SEARCHES

United States v. Forrester

In this case, the government had used a pen register analogue called a “mirror port.” This device enabled the government to collect the to/from addresses of defendant Alba’s e-mail messages, the IP addresses of the websites that Alba visited, and the total volume of information sent to or from his account. The Forrester court ruled that the surveillance did not constitute a Fourth Amendment search. The surveillance technique was indistinguishable for constitutional-purposes from the use of the pen register at stake in Smith v. Maryland.

The Forrester court also ruled that Alba was not entitled to any suppression of evidence, whether or not the computer surveillance was covered by the then applicable pen register statute. There is no mention of suppression of evidence in the pen register statute. This statute provides only for a fine or imprisonment for a knowing violation of it.

Note 1 – IP Addresses and URLs

This note asks whether IP addresses, as opposed to telephone numbers, are not constitutionally problematic. They certainly reveal more content-laden information than a list of telephone numbers, as in Smith v. Maryland.

Note 2 – Content vs. Envelope Information

Excerpts here set out a debate between Daniel Solove and Orin Kerr regarding the content versus envelope distinction. The law currently distinguishes between content and envelope information. Envelope information consists of data that involves to whom a communication is directed to and addressing and routing information. It is akin to the
information that would be found on the outside of an envelope. In contrast, content information consists of the content of a communication – the letter inside the envelope.

The law protects content information with strong protections (the Wiretap Act and the SCA) but it affords envelope information with very meager protections (the Pen Register Act). Solove questions whether such a distinction is tenable. In his view, people sometimes care more about preserving the confidentiality of the parties with whom they communicate rather than the privacy of the actual substance of the communication itself. Solove also contends that this dichotomy breaks down in the context of the Internet and IP addresses and URLs. Kerr takes issue with Solove’s argument, contending that for the most part, content information involves privacy concerns of a much greater magnitude than envelope information.

Note 3 – The Scope of the Pen Register Act

The USA Patriot Act expanded the definition of pen register to include DRAS-information, that is, “dialing, routing, addressing, or signaling information.” But it also explicitly excluded “the contents of any communication.” Some ambiguity still may exist, at least on the face of this amendment, regarding IP addresses and URL’s.

Note 4 – ECPA and the Exclusionary Rule

This note explores the issue of how electronic surveillance law ought to be enforced. Many provisions of electronic surveillance law lack an exclusionary rule, and Orin Kerr argues that the absence of such a judicial remedy leads to inadequate judicial attention to ECPA.

Note 5 – The Internet vs. the Telephone

Susan Freiwald contrasts the strong protection in the Wiretap Act of 1968 with ECPA’s weaker protection of online communications.
CHAPTER 2
NATIONAL SECURITY AND
FOREIGN INTELLIGENCE

SUMMARY OF MAJOR CHANGES FROM THE PREVIOUS EDITION

- We updated the note about the USA FREEDOM Act of 2015. At the time of the publication of the previous edition, various bills were still being considered by Congress. Congress eventually passed the USA FREEDOM Act to end the bulk collection of metadata under the USA-PATRIOT Act Section 215.

A. THE INTELLIGENCE COMMUNITY

This section sets out the various agencies in the U.S. intelligence community.

B. THE FOURTH AMENDMENT FRAMEWORK

The Court has long struggled over whether to treat the protection of national security differently from ordinary criminal investigations. This section explores the ambiguity and conflict on this issue.

**UNITED STATES v. UNITED STATES DISTRICT COURT (The “Keith” Case)**

The *Keith* case, *United States v. United States District Court*, is referred to as the *Keith* case because the federal district judge who originally heard it was Judge Damon Keith.

The case has an interesting background which is discussed in the casebook prior to the case. In 1969, the three founding members of a group called “the White Panthers” bombed a CIA office in Michigan. The group was not a white supremacist group; in fact, they supported the goals of the Black Panther Party. The group advocated that everything should be free and that money should be abolished. The group’s manifesto stated: “We demand total freedom for everybody! And we will not be stopped until we get it. . . . ROCK AND ROLL music is the spearhead of our attack because it is so effective and so much fun.”

During its investigation of the crime, the government wiretapped calls made by one of the bombers without a warrant or probably case as required by the Fourth Amendment. The wiretapping was not conducted with a warrant supported by probable cause as required by the Fourth Amendment.

The case made its way up to the U.S. Supreme Court in 1972. The Nixon Administration argued that because the bombing involved a threat to national security, it wasn’t bound by the Fourth Amendment. The government argued the U.S. Constitution grants the President
special national security powers to “preserve, protect and defend the Constitution of the United States,” and these powers trump the regular protections of the Fourth Amendment.

The U.S. Supreme Court rejected the argument by the Nixon Administration that the Fourth Amendment did not apply to matters of domestic national security, but it made some qualifications that created rather muddy waters in this area because the Court left so much unresolved.

Although the Fourth Amendment applies to domestic security, the Court noted that there may be “different” Fourth Amendment standards:

[D]omestic security surveillance may involve different policy and practical considerations from the surveillance of “ordinary crime.” The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. . . . Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government’s preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime. . . .

The Court also noted that foreign intelligence gathering within U.S. borders might not be governed by the Fourth Amendment:

[T]his case involves only the domestic aspects of national security. We have not addressed and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents but that surveillance without a warrant might be constitutional in cases where the target was an agent of a foreign power.

The rationale behind not applying the Fourth Amendment (or deviating from regular Fourth Amendment procedure) for foreign intelligence gathering is that the Fourth Amendment standards are focused on investigations of criminal activity. Probable cause is tied to suspicion of criminal activity. But foreign intelligence gathering often isn’t tied to criminal activity. The government just wants to learn what foreign agents are up to when in the United States, even if these agents are not engaged in criminal activity. Therefore, the warrant and probable cause standards do not fit well in this context.
Putting all this together, *Keith* establishes the following framework:

<table>
<thead>
<tr>
<th>CRIMINAL INVESTIGATIONS</th>
<th>Regular Fourth Amendment law applies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMESTIC NATIONAL SECURITY</td>
<td>The Fourth Amendment applies, but different standards (beyond a warrant and probable cause) may apply if they are reasonable.</td>
</tr>
<tr>
<td>FOREIGN INTELLIGENCE GATHERING</td>
<td>It remains an open question as to whether or how the Fourth Amendment applies. This area is now regulated by the Foreign Intelligence Surveillance Act (FISA).</td>
</tr>
</tbody>
</table>

**Note 1 – The Fourth Amendment Framework in *Keith***

Pointing to the difficulty in defining what precisely constitutes a “national security” issue, Daniel Solove argues that there should be no special treatment for national security surveillance. Richard Posner argues that the Fourth Amendment should adopt a “sliding scale” standard to allow for a lower level of suspicion in cases involving national security or crimes of great magnitude. Does a one-size-fits-all Fourth Amendment standard make sense? Should the same standard that applies to the investigation of a petty theft also apply to the investigation or prevention of a major terrorist attack?

**Note 2 – The Church Committee Report**

This note quotes from the **Church Committee Report**, which describes abuses by the FBI in national security surveillance, such as COINTELPRO.

**Note 3 – National Security vs. Civil Liberties**

Eric Posner and Adrian Vermeule have argued that the executive is the only organ of government with the “resources, power, and flexibility to respond to threats to national security.” Accordingly, they contend that courts should defer to the executive branch with regard to national security issues. This excerpt can lead to interesting discussions about the competence and role of each branch in handling national security issues.

**Note 4 – The Fourth Amendment and Foreign Intelligence Surveillance**

This note explores how the Fourth Amendment addresses foreign intelligence surveillance. The courts that have examined the question have decided that the Fourth Amendment does not require a warrant for foreign intelligence surveillance by the government.
C. FOREIGN INTELLIGENCE GATHERING

1. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

The Foreign Intelligence Surveillance Act (FISA) of 1978 establishes standards and procedures for use of electronic surveillance to collect foreign intelligence within the United States.

FISA has been the subject of much recent debate. FISA creates a different regime to govern surveillance to obtain “foreign intelligence” information. In contrast, federal electronic surveillance law covers domestic surveillance for all other purposes. Thus, ECPA applies to domestic law enforcement to govern the gathering of information for criminal investigations involving people in United States. FISA is designed primarily for intelligence gathering agencies to regulate how the government gains general intelligence about foreign powers within the borders of the United States.

FISA is very permissive. It provides for expansive surveillance powers with some judicial supervision, though that supervision is limited. FISA surveillance orders are issued by a secret court, which hears applications by the government ex parte. In practice, the FISA court has granted the vast majority of applications.

GLOBAL RELIEF FOUNDATION, INC. v. O’NEIL

This case is a good introduction to FISA. It illustrates the “emergency situation” provision of the statute. It also illustrates the “probable cause” requirement in FISA. Ordinarily, probable cause constitutes reasonable belief that a search will turn up evidence of criminal activity. In contrast, FISA’s probable cause requirement is that there must be probable cause that someone is an agent of a foreign power. There is no requirement that there be probable cause of any criminal activity.

FISA is much less stringent than the ECPA. This is because it does not apply to ordinary domestic investigations. The key triggers to FISA’s applicability are that the surveillance involve foreign powers or foreign agents and that the purpose of the surveillance be foreign intelligence gathering.

Note 1 – Probable Cause

This note explains how the required finding under FISA is different than under the Wiretap Act’s “super warrant.”

Note 2 – Defendants’ Rights?

FISA requires that defendants require notice of information derived from electronic surveillance pursuant to FISA when the government seeks to use the information at trial.
Note 3 – The Three Keith Categories

This note revisits the three categories established in the Keith case, discussed above. Domestic surveillance investigation, Keith category two, remains unregulated by Congress. As a result, law enforcement is required to carry out surveillance of criminal activities similar to those in Keith under the Wiretap Act, and other parts of ECPA as applicable.

Note 4 – The Lone Wolf Amendment

This note discusses the 2004 “Lone Wolf” amendments to FISA. In May 2011, President Obama signed a law containing a four-year extension of this provision. A lone wolf terrorist must be a non-U.S. person engaged in international terrorism, but need not be tied to a foreign power.

Note 5 – A New Agency for Domestic Intelligence?

Francesca Bignami discusses the assignment in Europe of responsibility to two agencies for gathering (1) information on threats posed abroad by foreign government, and (2) threats at home, whether from foreign powers or domestic threats. Richard Posner has criticized of the FBI’s being assigned authority over both (1) criminal investigations and (2) domestic intelligence.

United States v. Isa

This case has horrific facts – a wiretap carried out pursuant to FISA recorded the suspect’s murder of their sixteen-year-old daughter. The issue in the case is whether the FISA recording could be used in the criminal trial of the parents, as the FISA recording was carried out with much lesser requirements than the Fourth Amendment or ECPA.

The 8th Circuit refused to suppress the recording. It stated that FISA specifically authorized the retention of information that is “evidence of a crime.” The appellate court notes: “There is no requirement that the ‘crime’ be related to foreign intelligence.” In other words, evidence validly obtained under FISA can be used in an ordinary criminal prosecution.

This case emphasizes an important point about FISA: If in the course of gathering intelligence, officials discover evidence of a crime, they can turn it over to prosecutors to prosecute.

The fact that evidence obtained under FISA can be used in criminal prosecutions raises the issue of whether FISA could become an end-around of ECPA. In other words, the government could gather evidence under the much more lenient provisions of FISA (rather than the stricter ECPA provisions) and then turn it over to prosecutors to prosecute people. This is one of the reasons why the so-called “FISA wall” was developed.
Note 1 – Use of Information Obtained Through FISA Orders

FISA allows information obtained via its procedures to be used in a criminal trial — even though its standards are directed toward capturing of foreign intelligence information and not criminal activity. Instructors might ask whether such use should be permitted? Isa presents a stark example for this discussion. If using information captured under FISA were prohibited in criminal proceedings, then essential evidence about a murder would be excluded from trial. On the other hand, without the more relaxed standards of FISA, the government might not have been able to engage in the wiretapping, and thus such evidence might never have come into existence.

In Isa, the government happened to stumble upon the evidence – they weren’t using FISA to find out anything about the murder; it just happened to be captured during the wiretapping. The government didn’t use the laxer provisions of FISA as an end-run around ECPA.

The law attempted to strike a balance by using information screening “walls” to (1) allow sharing of information gleaned under FISA for criminal enforcement; and (2) prevent the use of FISA as an end-run around ECPA and the Fourth Amendment. Subsequent notes explore the “FISA wall,” its difficulties, and its breakdown.

Note 2 – Minimization Procedures and Information Screening “Walls”

This note discusses the “FISA wall,” which has often been blamed as being a factor in the failure of agencies to share information they had prior to 9/11. The “wall” is basically a way to prevent FISA from being used as an end-run around ECPA.

FISA sets forth intelligence gathering procedures, which are not tied to any suspicion that a crime is underway or planned or committed. Because information gathered validly under FISA can be used in a criminal prosecution, see United States v. Isa, what stops government officials from using the less protective provisions of FISA to gather information for use in a criminal investigation?

The “wall” is a set of procedures designed to provide this protection. It prevents those involved in the law enforcement or prosecution of crimes from becoming involved in the intelligence gathering at the beginning. Information can still be shared. The “wall” just prevents law enforcement officials from directing FISA investigations or using them in lieu of ECPA.

The difficult question is how terrorism investigations fit into the framework set out by FISA and ECPA. FISA and ECPA attempt to create a clear line between foreign intelligence gathering within the United States (covered by FISA) and domestic criminal investigations (covered by ECPA). The problem with terrorism is that it involves both foreign intelligence gathering and criminal investigation. Terrorism thus throws a wrench into the framework of Keith because it fits into all of the categories.
2. THE USA PATRIOT ACT

THE 9/11 COMMISSION REPORT

The 9/11 Commission Report points out the general confusion in the FBI regarding “the rules governing the sharing and use of information gathered in intelligence channels.” The Report presents a vivid concrete picture of intelligence gathering and terrorism investigations, and how a series of missteps led to failure to share important information that may have prevented the 9/11 attacks.

The Report points out that under FISA and the wall, the information should have been shared. But due to a purported misunderstanding of the law, officials failed to share the information.

Note 1—Confusion About the Law Before 9/11

This note asks whether the indications of law enforcement confusion about the wall point to a need for changes in FISA, changes in FBI training, or some other action. This material can lead to a discussion among students regarding how legal standards are best implemented within a law enforcement bureaucracy.

Note 2 – What Did the FISA “Wall” Require?

This note provides more background on the history of “wall” and examines the debate about the extent to which the “wall” presented a significant handicap for domestic intelligence investigations.

Note 3 – FISA and the USA PATRIOT Act

This note looks at the USA PATRIOT’s Act broadening of the applicability of FISA so it would apply when foreign intelligence gathering was “a significant purpose” of the investigation rather than “the purpose.” The idea behind the amendment was that an investigation could have mixed purposes; it could have both foreign intelligence and criminal goals. This change makes it easier to use FISA in these cases. The next decision, In Re Sealed Case, looks at this amendment to the FISA.

IN RE SEALED CASE

In re Sealed is the first published decision from the Foreign Intelligence Surveillance Court (FISC). Appeals from the FISC go to the Foreign Intelligence Surveillance Court of Review (FISCR). The FISCR rejected the lower court’s assumption that FISA constructed a barrier between counterintelligence/intelligences and law enforcement officials, i.e. the “wall.” It concedes that the Justice Department seems to have accepted this interpretation of FISA during the 1980’s, but finds this reading of the statute “puzzling.”

Moving from the 1978 FISA to the statute as amended in October 2001, the review court found “something of an analytic conundrum.” On the one hand, Congress did not amend
the definition of foreign intelligence information (including evidence of foreign intelligence crimes). On the other hand, Congress accepted the dichotomy between foreign intelligence and law enforcement by adopting the language of “a significant purpose” test (a significant purpose of the surveillance must be to obtain foreign intelligence information-- prior to the Patriot Act this language looked to “the purpose” of the surveillance). The court decided: “So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.” The importance of this part of the decision? “FISA, as amended, does not oblige the government to demonstrate to the FISA court that its primary purpose in conducting electronic surveillance is not criminal prosecution.”

Regarding the constitutionality of FISA, the appellate court found that “procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close.” Is coming close an adequate constitutional test-- even in circumstances involving national security?

**Note 1 – Assessing the Benefits and Problems of the “Wall”**

Peter Swire defends “the wall” as serving essential purposes. Swire also rejects the Patriot Act’s “significant purpose” test: “Under the new standard, an official could honestly affirm both a significant purpose for foreign intelligence and a likely use for law enforcement.” He views this Patriot Act amendment, as interpreted by the FISCR, as causing a slippery slope problem.

**Note 2 – The Constitutionality of FISA and the Protect America Act**

This note observes that the courts that looked at the constitutionality of FISA prior to the USA PATRIOT Act all concluded that it passed muster. It asks why there should be different constitutional standards under the Fourth Amendment for foreign intelligence and domestic law enforcement.

This note also discusses *In re Directives [redacted text]*, a 2008 decision of the Foreign Intelligence Surveillance Court of Review (FISCR). In it, the FISCR found that the PAA satisfied the requirements of the Fourth Amendment.

**Note 3 – After-the-Fact Reasonableness Review?**

A note in the Yale Law Journal by Nola K. Breglio proposes that the U.S. should repeal FISA and switch to warrantless foreign intelligence surveillance. Under this approach, targets would challenge the reasonableness of surveillance in an Article III court after the surveillance was completed. Most FISA surveillance presumably does not lead to charges against anyone, but is rather used for general counter-terrorism purposes. If the bulk of FISA scrutiny never leads to Article III cases, won’t this ex post enforcement approach lead to a lack of protection for vital interests?

**Note 4 – Stare Decisis**
The note discusses how stare decisis should work with secret opinions.

**Note 5 – The USA PATRIOT Act §215**

The provision of the USA PATRIOT amended FISA to permit the collection of “tangible things.” This authority was used by the NSA to justify its collection of bulk telephone metadata. Edward Snowden, a contractor for the NSA, first revealed the existence of this program in June 2014.

### 3. NATIONAL SECURITY LETTERS

National Security Letters (NSL) authority permits the FBI to obtain personal information from third parties by making a written request in cases involving national security. This section traces the different statutory bases for this legal authority and examines NSL litigation.

It is important to note that NSLs are different from the USA PATRIOT Act § 215. NSLs pre-dated § 215. There are several different NSL provisions:

1. ECPA’s Stored Communications Act – ISPs and phone companies must produce customer records
2. Right to Financial Privacy Act – records of banks and financial institutions
3. Fair Credit Reporting Act – information maintained by credit reporting agencies

The casebook discusses the litigation involving constitutional challenges to NSLs that has ensued over the past decade. This litigation is still ongoing. There are at least three potential constitutional problems with NSLs. First, they have a gag order on the recipient that might violate the First Amendment. Some courts have found the gag order provision to a prior restraint on free speech and to be too broad.

Second, NSLs are difficult to challenge in court, and courts have been troubled by how they impede judicial review.

Third, NSLs depart significantly from Fourth Amendment procedures. Although *Keith* allows for different Fourth Amendment procedures for matters of national security, they still must be “reasonable.” Are NSLs reasonable?

The courts are just starting to wrestle with these issues, and the casebook describes the litigation thus far.
4. INTERNAL OVERSIGHT

(a) The Attorney General’s FBI Guidelines

The surveillance activities of the FBI are regulated through constitutional strictures, electronic surveillance statutes, and Attorney General Guidelines. This Section considers the evolving nature of these guidelines as demonstrated by the revisions by Attorney General Ashcroft.

(b) The Homeland Security Act

This Act created a Privacy Officer for the new Department of Homeland Security.

(c) The Intelligence Reform and Terrorism Prevention Act

The Intelligence Reform and Terrorism Prevention Act increases the sharing of information within the United States Intelligence Community (USIC). This approach, if successful, will end the traditional “stovepiping” of information within the USIC. In addition, this Act set up a five-member Privacy and Civil Liberties Oversight Board. This Board has been the subject of controversy. After it got off to a slow start, the only Democratic member of it resigned once the Board issued its first report. His objection was to the editing of the report by the White House.

D. NSA SURVEILLANCE

The NSA has been involved in controversial activities in the United States. The first indication of these activities was a New York Times article in December 2005. This article discussed a program, which the Bush Administration later termed the “Terrorist Surveillance Program” (TSP). Other NSA activities may also have taken place.

In July 2008, Congress enacted the FISA Amendment Act (FAA), which establishes new rules for at least some of this NSA behavior. It also provides statutory defenses for the telecommunications companies that assisted the NSA.

All of these developments occurred pre-Snowden, who in 2013 leaked documents about extensive NSA surveillance.

1. STANDING

Clapper v. Amnesty International USA

In Clapper v. Amnesty International USA, various groups challenged a provision of FISA (§ 702) that authorized surveillance of non-United States persons reasonably believed to be outside of the U.S. The purpose of the surveillance was to gather foreign intelligence information. The plaintiffs, who are United States persons but who work with individuals outside of the country, argued that such authorization violated their constitutional rights
due to strong likelihood that the government would intercept their communications. The plaintiffs alleged that they therefore had to resort to costly measures in order to protect the confidentiality of such communications.

By a 5-4 majority, the Supreme Court held that the plaintiffs lacked Article III standing to bring the challenge. The Court held that they could not show future harm that was “certainly impending” and that their incurring of costs to protect the confidentiality of communications was not present harm capable of generating standing.

In dissent, Justice Breyer took issue with the majority’s reliance on the “certainty” requirement. He argued that federal courts have frequently found standing where the harm was “highly likely” rather than absolutely certain.

**Note 1 – The Holding in Clapper**

This note compares the majority’s and the dissent’s interpretation of the “certainly impending” requirement for standing. Is the requirement to allege certainty impending future harm justifiable in the national security context?

**Note 2 – The FISA Amendment Act and TSP**

In *Hepting v. AT&T*, plaintiffs alleged that they had suffered injury when AT&T worked with the NSA to conduct warrantless surveillance via the TSP program. The district court decided that the existence of TSP was not a secret for purposes of the states secret privilege.

However, the district court in *In Re NSA Telecommunications Records Litigation* granted the government’s motion to dismiss all claims against the “electronic communication services providers.” It retroactively granting immunity to the telecommunications company defendants based on the FISA Amendment Act of 2008. It found that this statute demonstrated an “unequivocal intention to create an immunity” for such defendants from liability in these actions.

**Note 3 – The End of FISA?**

*William Banks* calls for a restoration of the central terms of FISA. The Banks article predates the enactment of the FISA Amendment Act of 2008, discussed in the next note, and it would be interesting to ask a class if how it would evaluate this statute in terms of the reform that Banks desired. In contrast, *John Yoo* argues for use of data mining pursuant to FISA when there was “a 50 percent chance” or greater that terrorists would use a certain communication channel. Finally, *Orin Kerr* calls for an adding of “data-focused authorities” to FISA.

2. THE SNOWDEN REVELATIONS

This section summarizes the chief leaks of classified NSA material from Edward Snowden. The leaks revealed information about Section 702 surveillance, Section 215 surveillance, spying on the leaders of certain countries, and an attempt to weaken encryption standards.
The next two cases, *Klayman v. Obama* and *In re FBI*, concerned the legal sufficiency of Section 215 to permit the NSA’s activities under it.

**Klayman v. Obama**

*Klayman v. Obama* is helpful for its discussion of the Bulk Telephony Metadata Program carried out pursuant to Section 215. Plaintiffs challenged the constitutionality of provisions of FISA that authorized such governmental activity. The district court held that the plaintiffs had sufficient standing to challenge the provisions at issue because, in contrast to the plaintiffs in *Clapper*, they had more than merely speculative fear of surveillance. As customers of Verizon, a telecommunications provider confirmed to have been consistently providing its users’ data to the government, the plaintiffs were able to allege “strong evidence” that their particular communications had been collected.

The district court also held that the challenged surveillance likely violated the Fourth Amendment, but granted the government a stay to appeal the decision. The judge opined that *Smith v. Maryland* was not applicable precedent given changed present-day circumstances, particularly “the Government’s surveillance capabilities, citizens’ phone habits, and the relationship between the NSA and telecom companies.” Judge Leon flatly stated, “The question before me is not the same question that the Supreme Court confronted in *Smith*.”

**In re FBI**

As in *Klayman*, the plaintiffs in *In re FBI* challenged the constitutionality under the Fourth Amendment of the NSA’s bulk surveillance and collection of telephone metadata pursuant to the statutory authority granted by § 215. This court reached a contrary conclusion, however, holding that *Smith v. Maryland* applies to searches of telephone metadata, which excludes the content of the corresponding communications. The court relied on the content vs. non-content distinction established in *Smith* as well as the third party doctrine in holding that there was no reasonable expectation of privacy in the metadata collected by the government in this case. The FISC did point out one notable difference from the cited precedent: while the government accessed the pen register information of a sole individual suspected of a crime in *Smith*, the NSA orders at issue here required daily, indiscriminate collection of the information of a huge number of people. The distinction, however, was not persuasive for it.

Why did the FISC in *In re FBI* find Smith controlling while the district court in *Klayman* did not?

**Note 1 – Two Different Results: Klayman and In re FBI**

*Klayman* and *In re FBI* take far different approaches to *Smith v. Maryland*. *Klayman* finds four reasons that Smith is not controlling for the question of whether the NSA’s Bulk Telephony Metadata Program violated a reasonable expectation of privacy. First, the Smith pen register was only operational for a few days. In contrast, the NSA stored
metadata phone data for five years. Second, rather than just the phone company occasional sharing information with the government, as in Smith, the NSA and telephone companies had “a joint intelligence-gathering operation.” Third, the Klayman district court noted, “the almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979.” Finally, “and most importantly,” the court noted that “the nature and quantity of the information contained in people’s telephony metadata is much greater” than at the time of the Smith decision.

In re FBI finds “no legal basis” for the FISC to find other than that Smith controls. It states: “where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence ex nihilo.” Fourth Amendment rights are personal, and a widespread possible impingement of these rights are still to be assessed person-by-person.

At what point does a difference in degree necessarily become a difference in kind? Should lower courts wait for the Supreme Court to make that determination? Or, in light of the small number of decisions each year from the Supreme Court, should lower courts act on their perception of dramatically changed circumstances?

Note 2 – PCLOB on Section 215

PCLOB called for the end of the Telephony Bulk Metadata Program. It felt the program had serious implications for privacy and security. PCLOB also felt that the program failed to demonstrate its efficacy.

Note 3 – PCLOB on Section 702

In contrast to its negative views on the Telephony Bulk Metadata Program, PCLOB found that the Section 702 Program was a valuable part of the government’s efforts to combat terrorism. It also offered specific recommendations regarding this program.

It would be useful to lead a class discussion that contrasted the two programs and to explore the students’ assessment of them.

Note 4 – President’s Civil Liberties Review Board

Subsequent to the Snowden leaks, President Obama created a blue-ribbon panel, the President’s Review Group on Intelligence and Communications Technologies. This note discusses its recommendations.

Note 5 – Bulk Metadata: Private Sector or Governmental Control?

One possibility raised by the Review Board is to end storage of bulk meta-data by the government, but to let the telephone companies store it. PCLOB’s Rachel Brand felt that this approach would create more problems than it solved. One problem might be to
stimulate new demands for this data beyond national security. Another might be to raise liability issues for telephone providers holding it. Other unintended negative consequences of such an approach might be identified in a class discussion.

Note 6 – Caselaw on Section 702

The FISC has heard multiple cases involved the Section 702 program. This note discusses the major opinions from the FISC about it as well as a district court opinion upholding Section 702 against constitutional challenges.

Note 7 – Lack of Investigative Capacity

How should the FISC oversight be strengthened? Should it have some kind of audit function? How is its position different than that of other courts?

Note 8 – The USA FREEDOM Act

This note summarizes the USA FREEDOM Act of 2015, which ended the bulk collection of metadata under the USA-PATRIOT Act Section 215.