Privacy and Information Security Law

Randy Canis

CLASS 7

Privacy and Law Enforcement pt. 1

Privacy and Law Enforcement pt. 1

2

Privacy v. Security

- "One way that government promotes security is by investigating and punishing crimes. To do this, law enforcement officials must gather information about suspected individuals. Monitoring and information gathering pose substantial threats to privacy."

3

Constitutional Regulatory Regime

- The Fourth and Fifth Amendments significantly limit the government's power to gather information.
  - **4th** – "regulates the government's activities in searching for information or items as well as the government's seizure of things or people."
  - **5th** – "guarantees that '[n]o person . . . shall be compelled in any criminal case to be a witness against himself. …' The Fifth Amendment establishes a 'privilege against self-incrimination,' and it prohibits the government from compelling individuals to disclose inculpatory information about themselves."

4

A. THE FOURTH AMENDMENT AND EMERGING TECHNOLOGY

5

4th Amendment

- The right of the people to be secure in their persons, houses, papers, and effects, against **unreasonable searches and seizures**, shall not be violated, and no warrants shall issue, but upon **probable cause**, supported by oath or affirmation, and **particularly describing** the place to be searched, and the persons or things to be seized.

6

4th Amendment Issues

1) Is the government's information collecting regulated by the 4th Amendment?
2) Is the search or seizure reasonable?
3) What is the result of the 4th Amendment violation?

7

Applicability of Searches and Seizures

- 4th Amendment applies every time government officials conduct a "search" or "seizure" of an object, document or person

8

Reasonable Searches and Seizures

- The 4th amendment does not bar searches and seizures, but requires that they be "reasonable".
  - "Generally, a search or seizure is reasonable if the police have obtained a **valid search warrant**. To obtain a warrant, the police must go before a judge or magistrate and demonstrate that they have '**probable cause**' to conduct a search or seizure."

9

Scope of Search Warrants

- No unfettered search
  - "If the scope of the search exceeds that permitted by the terms of a validly issued warrant or the character of the relevant exception from the warrant requirement, the subsequent seizure is unconstitutional without more."

10

Exceptions to Warrant and Probable Cause Requirements

- Searches and seizures can be reasonable even without a warrant and probable cause
  - Impracticality, consent to search, "special needs" exception
  - *Terry* stops
  - Checkpoint and information seeking stops

11

Exclusionary Rule and Civil Remedies

- Redress for government official's violation of the 4th Amendment:
  - Suppression of evidence at a criminal trial ("exclusionary rule")
  - Civil remedy (1983 Action)

12

Subpoenas and Court Orders

- **Court orders** – information gathering mechanism specified by statute or regulations
- **Subpoena** – an order to obtain testimony or documents

13

Quashing

- "If the party served with the subpoena has an objection, she may bring a motion to quash or modify the subpoena."

14

Wiretapping, Bugging, and Beyond

- "A '**wiretap'** is a device used to intercept telephone (or telegraph) communications."
- "A '**bug'** is a device, often quite miniature in size, that can be hidden on a person or in a place that can transmit conversations in a room to a remote receiving device, where the conversation can be listened to."
- "A '**parabolic microphone**' can pick up a conversation from a distance. Typically, a small dish behind the microphone enables the amplification of sound far away from the microphone itself."

15

Electronic Surveillance

- "The Court has in the past sustained instances of 'electronic eavesdropping' against constitutional challenge, when devices have been used to enable government agents to overhear conversations which would have been beyond the reach of the human ear. … It has been insisted only that the electronic device not be planted by an unlawful physical invasion of a constitutionally protected area."
- Lopez v. United States

16

Katz v. United States

- Accused
  - Transmitting wagering information by telephone
- Manner Intercepted
  - Electronic listening and recording device attached to the outside of a public phone booth

17

Katz v. United States

- "[The Fourth] Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the **protection of a person's general right to privacy** — his right to be let alone by other people — is, like the protection of his property and of his very life, **left largely to the law of the individual States.**"

18

Katz v. United States

- "[T]he Fourth Amendment **protects people** — and not simply 'areas' — **against unreasonable searches and seizures** it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."

19

Katz v. United States

- "'Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,' and that **searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment** — subject only to a few specifically established and well-delineated exceptions…"

20

Katz v. United States

- "[F]irst that a **person have exhibited an actual (subjective) expectation of privacy** and, second, that the **expectation be one that society is prepared to recognize as 'reasonable.'** Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."

21

"Reasonable Expectation" or Privacy Test

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".

22

Berger v. New York

- "The **Fourth Amendment's** requirement that a warrant 'particularly describ(e) the place to be searched, and the persons or things to be seized,' repudiated these general warrants and '**makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another**. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'"

23

Berger v. New York

- "The purpose of the probable cause requirement of the Fourth Amendment [is] to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed…"

24

US v. Carpenter

- 2016 6th Cir.
- Issue
  - Use of cell site data without a warrant

25

US v. Carpenter

- "Timothy Carpenter and Timothy Sanders were convicted of nine armed robberies in violation of the Hobbs Act. The government's evidence at trial included business records from the defendants' **wireless carriers, showing that each man used his cellphone within a half-mile to two miles of several robberies during the times the robberies occurred**. The defendants argue that the government's collection of those records constituted a warrantless search in violation of the Fourth Amendment. In making that argument, however, the defendants elide both the distinction described above and the difference between **GPS tracking** and the far less precise locational information that the government obtained here. We **reject the defendants' Fourth Amendment** argument…"

26

US v. Carpenter

- "This case involves an asserted privacy interest in information related to personal communications. As to that kind of information, the federal courts have long recognized a core distinction: although the **content of personal communications is private, the information necessary to get those communications from point A to point B is not**."

27

US v. Carpenter

- "The Fourth Amendment protects the content of the modern-day letter, the email. … But courts have not (yet, at least) extended those protections to the internet analogue to envelope markings, namely the metadata used to route internet communications, like sender and recipient addresses on an email, or IP addresses."

28

US v. Carpenter

- [T]he cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves. The government's collection of business records containing these data therefore is not a search."

29

US v. Mattish

- 2016 E.D.VA
- Background
  - D charged with child pornography through use of "Playpen" operating on the Tor network
  - D argues against the investigative technique used against him

30

US v. Mattish

- "The Court FINDS, for the reasons stated herein, that probable cause supported the warrant's issuance, that the warrant was sufficiently specific, that the triggering event occurred, that Defendant is not entitled to a Franks hearing, and that the magistrate judge did not exceed her jurisdiction or authority in issuing the warrant. Furthermore, the Court FINDS **suppression unwarranted** because the Government did not need a warrant in this case. Thus, any potential defects in the issuance of the warrant or in the warrant itself could not result in constitutional violations, and even if there were a defect in the warrant or in its issuance, the good faith exception to suppression would apply."

31

US v. Mattish

- "[T]he Tor network possesses two primary purposes: (1) it allows users to **access the Internet in an anonymous fashion** and (2) it allows some websites - hidden services - to operate only within the Tor network. Although a website's operator usually can identify visitors to his or her site through the visitors' Internet Protocol ("IP") addresses, Tor attempts to keep a user's IP address hidden. … Because Tor attempts to keep users' IP addresses hidden, the Government cannot rely on traditional identification techniques to identify website visitors who utilize the Tor network."

32

US v. Mattish

- Playpen on the Tor network included a significant amount of child pornography and include information on child sexual exploitation
- "Upon registering for an account with Playpen, potential users were warned not to enter a real email address or post identifying information in their profiles."

33

US v. Mattish

- "In December 2014, a foreign law enforcement agency discovered Playpen and alerted the FBI. After locating Playpen's operator, the FBI executed a search of his home in Florida on February 19, 2015, seizing control of Playpen. **The FBI did not immediately shut Playpen down; instead, it assumed control of Playpen, continuing to operate it** from a government facility in the Eastern District of Virginia from February 20, 2015 through March 4, 2015."

34

US v. Mattish

- 2/20/15 - Magistrate judge authorizes "a network investigative technique ('NIT') on Playpen's server to obtain identifying information from activating computers identifying information from activating computers … It is undisputed that the FBI could not identify the locations of any of the activating computers prior to deploying the NIT. The NIT is a set of computer code that in this case instructed an activating computer to send certain information to the FBI."

35

US v. Mattish

- "Even though the warrant authorized the FBI to deploy the NIT as soon as a user logged into Playpen, SA Alfin testified that the Government did not deploy the NIT against Mr. Matish in this particular case until after someone with the username of 'Broden' logged into Playpen, arrived at the index site, went to the bestiality section - which advertised prepubescent children engaged in sexual activities with animals - and clicked on the post titled 'Girl 11YO, with dog.' **In other words, the agents took the extra precaution of not deploying the NIT until the user first logged into Playpen and second entered into a section of Playpen which actually displayed child pornography.** At this point, testified SA Alfin, the user apparently downloaded child pornography as well as the NIT to his computer. Thus, **the FBI deployed the NIT in a much narrower fashion than what the warrant authorized**."

36

US v. Mattish

- FBI issues a subpoena for information from the ISP
- ISP identifies the user
- Another judge authorizes a search warrant of the home
- "Pursuant to this second warrant, the FBI seized several computers, hard drives, cell phones, tablets, and video game systems."

37

US v. Mattish

- Law Enforcement Privilege
- "In order to illustrate that the privilege applies, the party 'must show that the documents contain information that the law enforcement privilege is intended to protect,' which 'includes information pertaining to law enforcement techniques and procedures, information that would undermine the confidentiality of sources, information that would endanger witness and law enforcement personnel [or] the privacy of individuals involved in an investigation, and information that would otherwise . . . interfere with an investigation.' … If 'the party asserting the privilege successfully shows that the privilege applies, the district court then must balance the public interest in nondisclosure against "the need of a particular litigant for access to the privileged information,"' as the privilege is qualified, not absolute. …"

38

US v. Mattish

- The defense also expects to 'challenge the government's case by arguing to the jury that child pornography found in the unallocated space of Mr. Matish's computer came from somewhere or someone else, or at least that the government cannot prove beyond a reasonable doubt that Mr. Matish intentionally downloaded illegal pictures.' []. To support this argument, Defendant relies on the supposition that 'the security settings on Mr. Matish's computer had been compromised by the government's NIT,' leaving his computer vulnerable to hackers and malware. …"

39

US v. Mattish

- "The Government alleges that disclosure of the code 'would be harmful to the public interest' because it 'could diminish the future value of important investigative techniques, allow individuals to devise measures to counteract these techniques in order to evade detection, [and] discourage cooperation from third parties and other governmental agencies who rely on these techniques in critical situations.' Doc. 56 at 22. Courts have held similar law enforcement techniques subject to the qualified privilege."

40

US v. Mattish

- "[A] magistrate considering whether probable cause supports the issuance of a search warrant simply must 'make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is **a fair probability that contraband or evidence of a crime will be found in a particular place**.' [] In order for a magistrate to conclude that probable cause exists, a warrant application's supporting **affidavit must be more than conclusory** and bare bones; indeed, the affidavit 'must provide the magistrate with a substantial basis for determining the existence of probable cause.'"

41

US v. Mattish

- "A court reviewing whether a magistrate correctly determined that probable cause exists should **afford the magistrate's determination of probable cause great deference**. … Therefore, 'the duty of a reviewing court is simply to ensure that the magistrate had a "substantial basis for . . . concluding] that" probable cause existed.'"

42

US v. Mattish

- "[I]t was not unreasonable for the magistrate judge to find that Playpen's focus on anonymity, coupled with Playpen's suggestive name, the logo of two prepubescent females partially clothed with their legs spread apart (or, as discussed below, the one scantily clad minor), and the affidavit's description of Playpen's content, **endowed the NIT Warrant with probable cause**. In fact, other courts have found that probable cause supported this exact NIT Warrant."

43

US v. Mattish

- "The Court FINDS that **no Fourth Amendment violation** occurred here because the Government **did not need a warrant to capture Defendant's IP address**. Therefore, even if the warrant were invalid or void, it was unnecessary, so no constitutional violation resulted from the Government's conduct in this case."

44

US v. Mattish

- "Generally, one has **no reasonable expectation of privacy in an IP address when using the Internet**. … This lack of a reasonable expectation of privacy stems from the fact that Internet users 'should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.' … The Ninth Circuit noted that 'IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.' …"

45

US v. Mattish

- "Even an Internet user who employs the Tor network in an attempt to mask his or her IP address lacks a reasonable expectation of privacy in his or her IP address. Presumably, one using the Tor network hopes for, if not possesses, a subjective expectation of privacy in his or her identifying information. Indeed, Tor markets itself as a tool to 'prevent[] people from learning your location . . .' See Tor Project: Anonymity Online, https://www.torproject.org (last visited May 24, 2016). However, **such an expectation is not objectively reasonable** in light of the way the Tor network operates."

46

US v. Mattish

- "It is clear to the Court that Defendant took great strides to hide his IP address via his use of the Tor network. However, the Court *FINDS* that **any such subjective expectation of privacy - if one even existed in this case - is not objectively reasonable**. SA Alfin testified that when a user connects to the Tor network, he or she must disclose his or her real IP address to the first Tor node with which he or she connects. This fact, coupled with the Tor Project's own warning that the first server can see '[t]his IP address is using Tor,' destroys any expectation of privacy in a Tor user's IP address."

47

US v. Mattish

- "Defendant's IP address was revealed in transit when the NIT instructed his computer to send other information to the FBI. The fact that the Government needed to deploy the NIT to a computer does not change the fact that Defendant has no reasonable expectation of privacy in his IP address. … Thus, the **Government's use of a technique that causes a computer to regurgitate certain information, thereby revealing additional information that the suspect already exposed to a third party - here, the IP address - does not represent a search** under these circumstances. Therefore, the Government did not need to obtain a warrant before deploying the NIT and obtaining Defendant's IP address in this case, so any potential defects in the warrant or in the issuance of the warrant are immaterial."

48

US v. Mattish

- "[T]he Government obtained a traditional residential search warrant before searching the computer's contents in this case. Plus, Defendant lacked any expectation of privacy in the main piece of information the NIT allowed the FBI to gather - his IP address. … Additionally, while the Government could have deployed the NIT as soon as a user logged into Playpen, SA Alfin testified that in this particular case, the FBI took the extra step of not deploying the NIT until after the suspect actually accessed child pornography. These facts support the conclusion that the **NIT's deployment does not represent a prohibited search under the Fourth Amendment**."

49

Misplaced Trust Doctrine

- "[P]eople place their trust in others at their own peril and must assume the risk of betrayal."

50

Smith v. Maryland

- Accused
  - Victim robbed
  - Threatening phone calls made to victim and home drive byes
  - Traced license plate of car
  - Installed a pen register without a warrant
  - Searched accused home and uncovered additional evidence tying accused to robbery

51

Smith v. Maryland

- "[T]his Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action. This inquiry … normally embraces two discrete questions. The first is whether the individual, by his conduct, has '**exhibited an actual (subjective) expectation of privacy**,' — whether… the individual has shown that 'he seeks to preserve [something] as private.' The second question is whether the individual's subjective expectation of privacy is one that society is prepared to recognize as 'reasonable,' — **whether … the individual's expectation, viewed objectively, is 'justifiable' under the circumstances**."

52

Smith v. Maryland

- "Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is **too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret**."

53

Smith v. Maryland

- "[E]ven if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as 'reasonable.'"

54

Pen Register and Trap and Trace Decives

- **Pen register** – records outgoing telephone calls
- **Trap and trace device** – records incoming telephone calls

55

Bank Records

- Bank must report every deposit, withdrawal, or other transfer of currency exceeding $10,000
- Transactions exceeding $5,000 into or out of the United States must also be reported
- 31 U.S.C. §1081

56

Privacy and the Mail

- 4th Amendment protects the contents of a sealed letter but not the outside
- The government can search letters sent from abroad

57

Items Exposed to the Public

- "The warrantless search and seizure of the **garbage bags left at the curb** outside the Greenwood house would violate the Fourth Amendment only if respondents manifested a subjective expectation of privacy in their garbage that society accepts as objectively reasonable. … [W]e conclude that respondents exposed their garbage to the public sufficiently to **defeat their claim to Fourth Amendment protection**."
- California v. Greenwood (1988)

58

Plain View Doctrine

- "[I]t has long been settled that objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence."
- Harris v. United States, 390 U.S. 234, 236 (1968).

59

Open Fields Doctrine

- "An individual does not have a reasonable expectation of privacy in the open fields that she owns."
- "Under the **curtilage doctrine**, parts of one's property immediately outside one's home do not fall within the open fields rule. This exception does not mean that the curtilage is automatically afforded Fourth Amendment protection; a reasonable expectation of privacy analysis still must be performed."

60

Fenced In Areas

- We recognized that the yard was within the curtilage of the house, that a fence shielded the yard from observation from the street, and that the occupant had a subjective expectation of privacy. We held, however, that such an expectation was not reasonable and not one 'that society is prepared to honor.' Our reasoning was that **the home and its curtilage are not necessarily protected from inspection that involves no physical invasion.** ""What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.""
- Florida v. Riley, 488 U.S. 445 (1989)

61

Aerial Photographs

- But the photographs here are not so revealing of intimate details as to raise constitutional concerns. Although they undoubtedly give EPA more detailed information than naked-eye views, they remain limited to an outline of the facility's buildings and equipment. … We hold that the taking of **aerial photographs** of an industrial plant complex **from navigable airspace is not a search** prohibited by the Fourth Amendment. …"

62

Warrantless Searches of Homes

- "With few exceptions, the question whether a **warrantless search of a home** is reasonable and hence constitutional must be answered **no**."

63

Thermal Imager

- "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," [] constitutes a search — at least where (as here) the technology in question is not in general public use. …On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search."
- Kyllo v. United States, 533 U.S. 27 (2001)

64

United States v. Jones

- Issue
  - Use of GPS tracking device on a vehicle to monitor movements on public streets is a search or seizure within 4th Amendment

65

United States v. Jones

- "We hold that the Government's installation of a **GPS device** on a target's vehicle, and its use of that device to monitor the vehicle's movements, **constitutes a 'search.'**"

66

Drug Sniffing Dogs

- "[T]he use of a **drug-sniffing dog** on a homeowner's porch to investigate the contents of the home was a '**search**' within the meaning of the Fourth Amendment."

67

B. INFORMATION GATHERING ABOUT FIRST AMENDMENT ACTIVITES

68

Seizure of Books

- "[T]he constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the **most scrupulous exactitude** when the 'things' are **books**, and the basis for their seizure is the ideas which they contain. No less a standard could be faithful to First Amendment freedoms."
- Stanford v. Texas, 379 U.S. 476 (1965)

69

Privacy Protection Act

- The PPA prohibits government officials from **searching or seizing work product** materials or documents 'possessed by a person reasonably believed to have a **purpose to disseminate to the public** a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce.' However, if 'there is probable cause to believe that the **person possessing such materials has committed or is committing the criminal offense** to which the materials relate,' then such materials may be searched or seized.

70

Gonzales v. Google

- Issue
  - Subpoena of Google for URL samples and all search engine queries for a two month time period
  - Narrowed twice to sample of 50K URLS

71

Gonzales v. Google

- "Given the broad definition of relevance in Rule 26, and the current narrow scope of the subpoena, despite the vagueness with which the Government has disclosed its study, the Court gives the Government the benefit of the doubt. The Court finds that **50,000 URLs randomly selected** from Google's data base for use in a scientific study of the effectiveness of filters is **relevant** to the issues in the case of *ACLU v. Gonzales*."

72

Gonzales v. Google

- "What the Government has not demonstrated, however, is a substantial need for *both* the information contained in the **sample of URLs** and sample of **search query text**. Furthermore, even if the information requested is not a trade secret, a district court may in its discretion limit discovery on a finding that 'the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive.' Rule 26(b)(2)(i).

73

Gonzales v. Google

- The court allows for the URL samples but not the search queries themselves…

74

C. FEDERAL ELECTRONIC SURVEILLANCE LAW

75

47 U.S. Code §605 - Unauthorized publication or use of communications

(a) Practices prohibited

Except as authorized by chapter 119, title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign **communication by wire or radio shall divulge or publish** the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception,

(1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority.

No person not being authorized by the sender **shall intercept** any radio communication and divulge or **publish** the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress, or which is transmitted by an amateur radio station operator or by a citizens band radio operator.

76

Applicability

- States could still use evidence in violation of §605 (while the Federal government could not)
- §605 only applied to wire communications and wiretapping and not eavesdropping on non-wire communications

77

Title III

- Applied to wiretaps by Federal and State officials
- Required Federal agents to apply for a warrant before wiretapping
- Criminalized private wiretapping
- No violation if one party consents

78

Electronic Communications Privacy Act (ECPA)

1) Wiretap Act
   - Communications in transmission
2) Stored Communication Act (SCA)
   - Communications in storage
3) Pen Register Act

Passed in 1986; amended Title III

79

4th Amendment?

- "Electronic surveillance law operates independently of the Fourth Amendment. Even if a search is reasonable under the Fourth Amendment, electronic surveillance law may bar the evidence. Even if a search is authorized by a judge under federal electronic surveillance law, the Fourth Amendment could still prohibit the wiretap."

80

Communication Classifications Under ECPA

- Wire Communications
- Oral Communications
- Electronic Communications

81

Wire Communications

- "**wire communication**" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce
- 18 U.S. Code §2510(1)

82

Oral Communications

- "**oral communication**" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication
- 18 U.S. Code §2510(2)

83

Electronic Communications

"**electronic communication**" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device []; or

(D)electronic funds transfer information [];

18 U.S. Code §2510(12)

84

Not Protected by the Exclusionary Rule

- Electronic communications are not protected by the exclusionary rule in the Wiretap Act or the Stored Communications Act
- Wire or oral communications that fall within the Stored Communications Act

85

Wiretap Act

- Except as otherwise specifically provided in this chapter any person who—
- (a) **intentionally intercepts**, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
- (b) **intentionally uses**, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—
  - (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
  - (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
  - (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; …

86

Wiretap Act (cont'd)

- (c) **intentionally discloses**, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, **knowing** or having reason to know that the information was **obtained through the interception** of a wire, oral, or electronic communication in violation of this subsection;
- (d) **intentionally uses**, or endeavors to use, the contents of any wire, oral, or electronic communication, **knowing** or having reason to know that the information was **obtained through the interception** of a wire, oral, or electronic communication in violation of this subsection…
- 18 U.S.C. §2511(1)

87

Exclusion/Penalty

- Can move to exclude wire or oral communications
- Violations of Wiretap Act - 10K per violation plus up to 5 years imprisonment

88

Exceptions

1) When one party to the communication consents
2) Communication service providers :to intercept, disclose, or use that communication in the normal course of [] employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service"

89

Stored Communications Act

(a) Offense.—Except as provided in subsection (c) of this section whoever—

(1) **intentionally accesses** without authorization a facility through which an electronic communication service is provided; or

(2) **intentionally exceeds an authorization** to access that facility;

and thereby obtains, alters, or prevents authorized **access to a wire or electronic communication while it is in electronic storage** in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. §2701

90

In re Yahoo Mail Litigation

- N.D.CA 2016
- Issue
  - Litigation regarding Yahoo's "interception, storage, reading and scanning of email violates Plaintiffs' and other consumers' rights of privacy."
  - Approval of a settlement agreement regarding Yahoo!'s scanning of email

91

In re Yahoo Mail Litigation

- Yahoo agrees to change its email architecture
- [District] Court [] found that Yahoo's terms of service 'establish[] [that] Yahoo Mail users[] consent[ed] to Yahoo's practice of scanning and analyzing emails for the purposes of creating user profiles for both parties to the email communication and sharing content from the emails with third parties.'"

92

In re Yahoo Mail Litigation

- "Of Plaintiffs' claims, only Plaintiffs' claim under §2702(a)(1) of the Stored Communications Act ('SCA') and under §631 of the California Information Privacy Act ('CIPA') survived Yahoo's motion to dismiss. Id. at 1043. The thrust of Plaintiffs' SCA and CIPA claims is that **'Yahoo intercepts and scans . . . incoming [and outgoing] emails for content during transit and before placing the emails into storage**.'"

93

In re Yahoo Mail Litigation

- "The Settlement Agreement provides Plaintiffs the relief that Plaintiffs seek under both the SCA and CIPA: **Yahoo will now only analyze emails for content when these emails are no longer in transit and after these emails reach a Yahoo Mail user's inbox or outbox**."

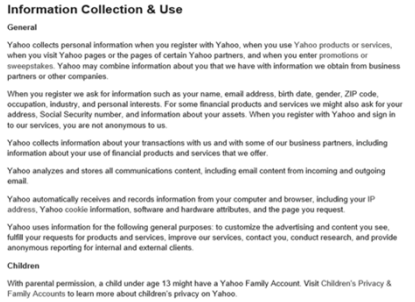
94

Yahoo! Terms of Service and Privacy Policy

- Yahoo Terms of Service
  - https://policies.yahoo.com/us/en/yahoo/terms/utos/index.htm
- Yahoo Privacy Policy
  - https://policies.yahoo.com/us/en/yahoo/privacy/index.htm

95

Yahoo! Privacy Policy



Information Collection & Use

General

Yahoo collects personal information when you register with Yahoo, when you use Yahoo products or services, when you visit Yahoo pages or the pages of certain Yahoo partners, and when you enter promotions or sweepstakes. Yahoo may combine information about you that we have with information we obtain from business partners or other companies.

When you register we ask for information such as your name, email address, birth date, gender, ZIP code, occupation, industry, and personal interests. For some financial products and services we might also ask for your address, Social Security number, and information about your assets. When you register with Yahoo and sign in to our services, you are not anonymous to us.

Yahoo collects information about your transactions with us and with some of our business partners, including information about your use of financial products and services that we offer.

Yahoo analyzes and stores all communications content, including email content from incoming and outgoing email.

Yahoo automatically receives and records information from your computer and browser, including your IP address, Yahoo cookie information, software and hardware attributes, and the page you request.

Yahoo uses information for the following general purposes: to customize the advertising and content you see, fulfill your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients.

Children

With parental permission, a child under age 13 might have a Yahoo Family Account. Visit Children's Privacy & Family Accounts to learn more about children's privacy on Yahoo.

96

Yahoo! Privacy Policy

Information Sharing & Disclosure

Yahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:

- We provide the information to trusted partners who work on behalf of or with Yahoo under confidentiality agreements. These companies may use your personal information to help Yahoo communicate with you about offers from Yahoo and our marketing partners. However, these companies do not have any independent right to share this information.
- We have a parent's permission to share the information if the user is a child under age 13. See Children's Privacy & Family Accounts for more information about our privacy practices for children under 13.
- We respond to subpoenas, court orders, or legal process (such as law enforcement requests), or to establish or exercise our legal rights or defend against legal claims.
- We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo's terms of use, or as otherwise required by law.
- We transfer information about you if Yahoo is acquired by or merged with another company. In this event, Yahoo will notify you before information about you is transferred and becomes subject to a different privacy policy.

Yahoo displays targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click targeted ads meet the targeting criteria—for example, women ages 18-24 from a particular geographic area.

- Yahoo does not provide any personal information to the advertiser when you interact with or view a targeted ad. However, by interacting with or viewing an ad you are consenting to the possibility that the advertiser will make the assumption that you meet the targeting criteria used to display the ad.
- Yahoo advertisers include financial service providers (such as banks, insurance agents, stock brokers and mortgage lenders) and non-financial companies (such as stores, airlines, and software companies).

Yahoo works with vendors, partners, advertisers, and other service providers in different industries and categories of business. For more information regarding providers of products or services that you've requested please read our detailed reference links.

97

In Class Discussion

- Feelings about Yahoo! Privacy Policy
- Would you understand how your personal information is being used, and how information is being collected from you?

98

Exclusion/Penalty

- Can move to suppress wire or oral communications
- Violations of Stored Communications Act - 1K per violation plus up to 6 months of imprisonment

99

Pen Register Act

- "Subject to certain exceptions, 'no person may install or use a pen register or a trap and trace device without first obtaining a court order.'"
- 18 U.S.C. §3121(a)

100

Pen Register

- the term "**pen register**" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business
- 18 U.S.C. §2137(3)

101

Exclusion/Penalty

- Cannot move to suppress material from violations of Pen Register Act
- Violations of Pen Register Act – fined plus up to one year of imprisonment

102

CALEA/ Digital Telephony Act

- The Communications Assistance for Law Enforcement Act (CALEA) of 1994 a/k/a "Digital Telephony Act
- Requires telecomm providers to help facilitate the government in executing legally authorized surveillance
- Does not apply to email and Internet access; FCC declared applies to VOIP

103

USA Patriot Act

- Congress passed in response to 9/11
- Sweeping law expanding government's surveillance powers

104

Delayed Notice of Search Warrants

- 4th Amendment – gov't must **obtain a search warrant and provide notice** before conducting a search or seizure
- §3103(a) addition – "enabling the government to **delay notice** if the court concludes that there is 'reasonable cause' that immediate notice will create an 'adverse result' such as physical danger, the destruction of evidence, delayed trial, flight from prosecution, and other circumstances."

105

Pen Registers

- "These changes altered the definition of a pen register from applying not only to telephone numbers but also **to Internet addresses, e-mail addressing information** (the 'to' and 'from' lines on e-mail), and the **routing information** of a wide spectrum of communications. The inclusion of 'or process' after 'device' enlarges the means by which such routing information can be intercepted beyond the use of a physical device. … The person whose communications are subject to this order **need not even be a criminal suspect**; all that the government needs to certify is relevance to an investigation."

106

State Electronic Surveillance Law

- 1 party consent or all party consent?
- First amendment issues?

107

Program Completed

108