The Wiretap Act
(Chapter 6A)

Sookhyun Yang
Statutory Privacy Laws

• In a network environment, the Fourth Amendment protections are supplemented by a set of federal statutory privacy laws.

• The major purpose of statutory privacy laws is to regulate efforts by criminal investigators to collect evidence that can help them identify a criminal.
  – The Stored Communication Act (18 U.S.C. §§2701-11) regulates access to stored content and non-content records held by ISPs.
    • Example) an FBI agent issues a subpoena ordering an ISP to disclose basic subscriber information about a particular Internet account.
Brief History

• 1928: The opinion for the Court invited Congress to enact statutory prohibitions on telephone wiretapping.

• The Communication Act of 1934
  – “No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person.”

• The Wiretap Act (a.k.a. Title III) of 1968
  – The statute regulates both government actors and private parties and it imposes strict limitations on the use of devices to intercept “oral communications” or “wire communications”
  – It also allows the government to obtain court orders permitting interception when investigators have probable cause and can satisfy a number of additional requirements.
  – The requirements of Title III beyond the usual search warrant requirement have led some to describe Title III intercept orders as “super warrants.”

• The Electronic Communications Privacy Act (ECPA) of 1986
  – The Wiretap Act was extended to “electronic communications (broadly computer communications).”
  – The Stored Communications Act was created.
  – The Pen Register Statute was created only for telephone calls.

• The Patriot Act of 2001
  – The Pen Register Statute was expended to the Internet.
Statutory Suppression Remedy

• The Fourth amendment is enforced with an exclusionary rule.

• However, the statutory privacy laws do not include a statutory suppression remedy in the “computer context.”
  – The only statutory suppression remedy is for violations of the Wiretap Act involving the interception of human voice communications.
  – The rationale in 1986 was that computer communications implicated lesser privacy concerns than telephone calls and speech involving the human voice.

• Currently (2003) the law lacks a statutory suppression remedy for communications other than voice communications.
Basic Structure of the Wiretap Act

- Prohibits the real-time interception of “content” of any wire, oral, or electronic communications, unless an exception applies or investigators have a “super warrant” interception order.
  - The statute envisions an individual is exchanging communications with another person or machine.
  - §2510 (4) defines “intercept”
  - §2510 (8) defines “content”
  - Three exceptions: the consent exception §2511(2)(c)-(d), the provider exception §2511(2)(a)(i), and the computer trespasser exception §2511(2)(i).
  - §2512 prohibits possessing or distributing wiretapping devices.
  - §2513 involves the forfeiture of such devices.
  - §2514 has been repealed.
  - §2516 lays out Title III intercept “super warrant.”
  - §2517 concerns the use and disclosure of the fruits of wiretapping.
  - §2519 requires the filing of annual reports on government wiretapping practices.
  - §2520 permits civil damages for unlawful wiretapping.
  - §2521 permits injunctions in civil cases.
  - §2522 involves compliance with the CALEA (Communication Assistance for Law Enforcement)

- Makes it a crime for someone who is not a party to the communication to intercept content in real-time.
Three Distinct Types of Communications

- **Wire communications §2510 (1), (18)**
  - Are communications that contain the human voice and that are sent over a wire
  - Examples: telephone calls, VOIP

- **Oral communications §2510 (2)**
  - Are “in person” recordings of the human voice that can be picked up by a bugging device or microphone when the person recorded has a reasonable expectation of privacy

- **Electronic communications §2510 (12)**
  - Are communications that do not contain the human voice
  - Include almost all computer transmissions.
O’BRIEN v. O’BRIEN in 2005

• What happened?
  – The Husband got temporal and permanent injunction to prevent the Wife from disclosing the communications.
  – The Husband also granted a request that the trial court preclude introduction of the communications into evidence in the divorce proceeding.

• The Wife’s motion for rehearing, which is subsequently denied
  – The electronic communications do not fall under the umbra of the Wiretap Act because these communications were retrieved from storage and therefore, are not “intercepted communications. The communications were stored before acquisition because once the text image became visible on the screen, the communication was no longer in transit, and therefore, not subject to intercept.
O’BRIEN v. O’BRIEN in 2005

• Here, the core of issues is:
  – 1) A distinction between “what is transmitted subject to interception” and “the storage of what has been previously communicated.”
  – 2) Whether the improperly intercepted electronic communications may be excluded from evidence under the exclusionary provisions of the Act.

• **Steiger case**
  – The hacker received pornographic material from the computer to the hacker’s computer using the Trojan horse virus which copied information that had previously been stored on the computer’s hard drive.
  – Decision: In this case, the capture of the electronic communication was not an interception.
  – Decision: Interception could occur if the virus or software intercepted the communications as being transmitted and copied it.

• **Final decision of O’BRIEN v. O’BRIEN**
  – 1) The Wife intercepted the electronic communications *contemporaneously with transmission*, copied it, and routed the copy to a file in the computer’s hard drive.
  – 2) The trial court found that the electronic communications are illegally intercepted in violation of the Act and ordered they not be admitted in evidence.
Content vs. Non-content

• Based on §2510 (8), content … includes any information concerning the substance, purport, or meaning of that communication.

• Ambiguous examples on content of communications
  – URL
  – The user’s command for retrieving web-pages
  – The communication between an operator and a speaker for placing the call request
  – The hacker’s communication for attempting to take over a remote server
  – Post-cut-through dialed digits
Consent Exception

• A person **acting** under color of law is one of parties to communications or has prior consent given from one of parties to communications.
  
  − A person acting under color of law is a private person jointly engaged with state officials in the prohibited action…

• A person **not acting** under color of law is one of parties to communications or has prior consent given from one of parties to communications unless communication is intercepted for crime or tortious act.

• **GRIGGS-RYAN v. SMITH (1990)**
  
  − Smith (a landlady) suspected plaintiff (a tenant)’s friend of offensive overtures and informed plaintiff on a number of occasions that all calls to her home were being tape-recorded.
  
  − Smith overheard and recorded plaintiff’s conversation on a drug transaction and disclosed overheard conversation to the police.
  
  − Based on a recorded conversation, a policeman got a warrant to search plaintiff’s abode and arrested plaintiff for marijuana and trafficking.
Decision of GRIGGS-RYAN v. SMITH

• A suppression hearing in the state superior court
  – Plaintiff was “unaware” of Smith’s eavesdropping.
  – Therefore, Smith’s recording was inadmissible.
  – The judge suppressed the fruits of the search.

• The instant suits in federal court
  – Based on Smith’s warning on monitoring, Smith argued that plaintiff effectively acquiesced in the interception.
  – The distinct court held Plaintiff’s receiving of a telephone call inside of Smith’s home manifests implied consent sufficient to trigger the prior consent exception.
Provider Exception

• Unlike other Wiretap Act exceptions, the provider exception regulates both the interception and the disclosure of communications, and both steps must be independently justified.

• US v. AULER
  – Auler bypassed the telephone company’s billing equipment using a blue box.
  – Two telephone company security agents detected Auler’s use of a blue box and informed an FBI agent.
  – An FBI agent got a warrant to search Auler’s house and accompanied with the security supervisors.
  – An FBI agent seized a blue box in Auler’s house.
Decision of US v. AULER

• Auler’s argument: Telephone company’s surveillance of his conversations extended beyond the scope of permissible interception.
  – Telephone company only disclosed to the FBI the limited evidence reasonably permitted.

• Auler’s argument: The search warrant, executed by the FBI was obtained as a result of illegal surveillance directed by Government agents.
  – The FBI neither initiated nor directed the surveillance conducted by telephone company. The surveillance had been conducted independently of any governmental direction.
McCLELLAND v. McGRATH

• **What happened?**
  – McClelland is a kidnapper.
  – The officers asked telephone company to trace ransom calls.
  – The telephone company informed officers that ransom calls had been made on a “cloned” phone.

• **Decision: Prosecution was terminated.**
  – McClelland filed a complaint that the officer’s interception is against the Wiretap Act.
  – The defendants moved to dismiss the complaint on the ground of provider exception by stating a criminal phone was cloned.
  – However, officers are not free to ask or direct telephone company to intercept any phone calls or disclose their contents, …It seems clear that telephone company was motivated by its desire to help the officers rather than to protect its own property, …
Computer Trespasser Exception

- The government can intercept the computer trespasser’s communications with the victim’s permission, so long as the government is already conducting an investigation.
  - §2511(21) defines “computer trespasser.”
    - Means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; AND
    - ...

- This exception clarified whether computer owners could obtain the assistance of law enforcement in conducting such monitoring.
  - Allows victims to authorize persons “acting under color of law” to monitor trespassers on their computer systems.
Honeypot

- Does the use of honey pots by a computer security professional violate the Wiretap Act?
- Can we justify monitoring intrusion into honey pot under the consent exception, under the provider exception or under trespasser exception?
- What if a criminal investigator wishes to set up a honey pot to identify intruders?