



*Sysadmins, Network Managers  
and wiretap law*

If you think your job sucks,  
imagine Federal Prison.



# Disclaimer

---

- This talk discusses current U.S. Federal law. Each U.S. State has its own laws that may differ from Federal law.
- This is not legal advice. I am an attorney, but I'm not your attorney.
- This area of law is in flux. What's legal today may change next month.



# Acknowledgments

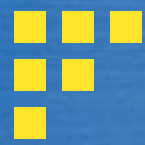
---

This research would not have been completed  
without help from:

Temple University Beasley School of Law

The Circuit Executive's Office of the U.S.  
Court of Appeals for the Third Circuit

The organizers of LISA 2006



# Overview

---

- What content may an admin look at on their network, and when?
- What is protected traffic, and what is not?
- How can you protect yourself and your organization from legal troubles?



# Competing Laws

---

- 4th amendment, U.S. Constitution
- Wiretap / Electronic Communications Privacy Act (18 U.S.C §§ 2510-2522)
- Stored Communications Act (18 U.S.C. §§ 2701-2711)
- Pen Register/ Trap and Trace (18 U.S.C. § 3121)
- State and Local statutes and common law



# 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...”
- Does not apply to non-government actors, unless acting as agent of the State
- However, some states allow civil suits for ‘intrusion into seclusion’ by private actors



# The changing 4<sup>th</sup> Amendment view of electronic communications

---

- *Olmstead v US* (1928) (broadcast view)
  - Wiretap w/o warrant not unreasonable, as “The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment.”



# The changing 4<sup>th</sup> Amendment view of electronic communications

---

- *Katz v US* (1967) (current view)
  - Wiretap is search, which requires warrant
  - “My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first 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.” Harlan, J.





# What communications are protected under the 4<sup>th</sup> Amendment?

---

- Receiving (but not transmitting) communication
  - Hoffa v U.S. (no protection of transmitted communication since any recipient may be informant)
- Information that must be given to third parties- no protection
  - e.g. Address on package



# Wiretap/ECPA Title 1

---

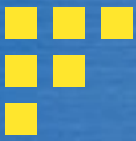
- Wiretap law originally enacted in Omnibus Crime Control act of 1968
- Significantly updated in 1986 by ECPA
- Updated again in 2001 by PATRIOT act
- FISA (50 USC § 1801 et seq) is of recent interest



# Wiretap Act

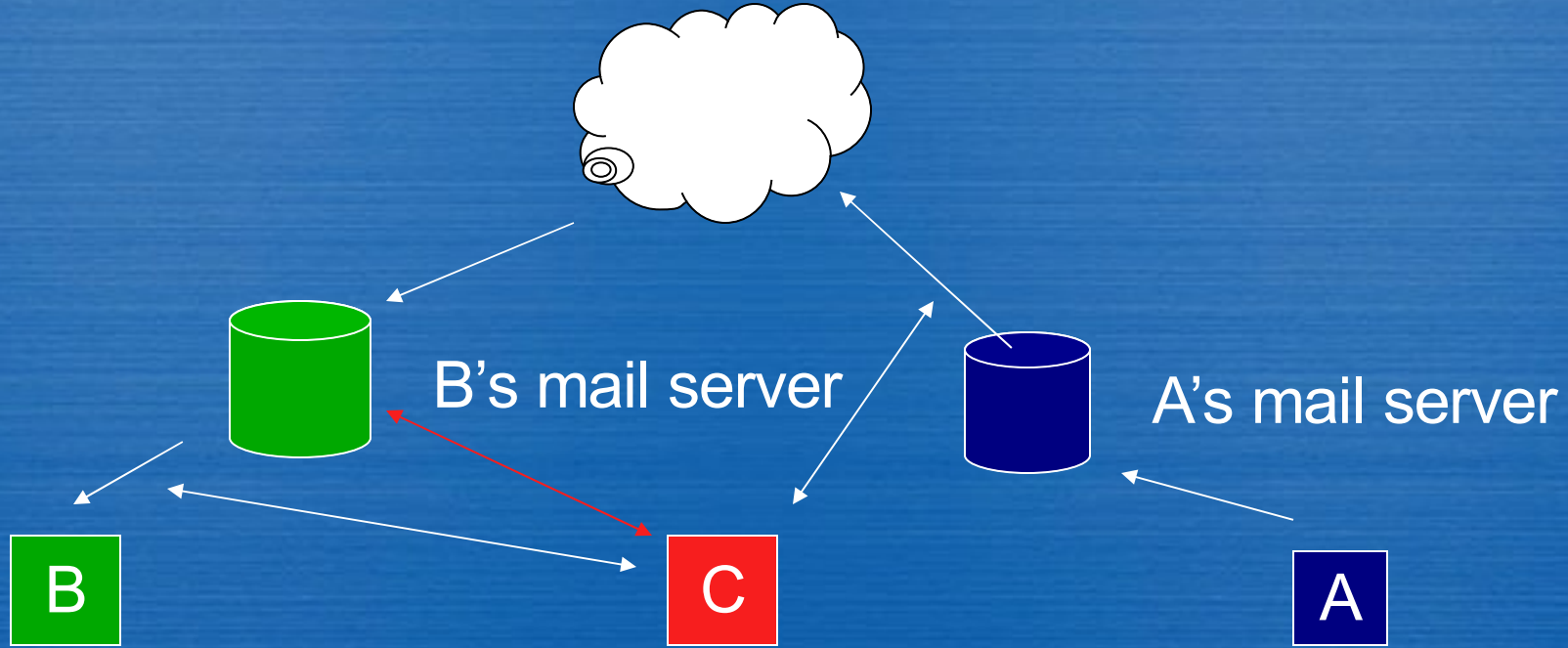
---

- “Interception” : acquisition of the **contents** of any ..., electronic, or oral communication through the use of any ... device. 18 USC § 2510
- Interception only when contemporaneous with transmission- not from storage (Steve Jackson Games v Secret Service)
- Federal prison up to five years, and victims may sue for damages and legal fees
- Evidence obtained under illegal interception inadmissible in court 18 USC § 2510(10)(a)



# What does interception look like?

A is sending email to B  
C wants to read the email before B does





# Interception exceptions

---

- Recipient (intended recipient of communication)
- Service provider agents and employees, to provide service, to protect the rights or facilities of the service provider, to comply with a court order or wiretap order or with the permission of the user
- To determine the source of harmful electronic interference
- To lawfully investigate a computer trespasser with the owner's consent, provided that no innocent communications are intercepted
- Pursuant to a valid FISA court order or Title III wiretap warrant



# Stored Communications Act

- Accessing a ‘stored communications service’ without permission or exceeding granted permissions and obtains, alters or prevents authorized access to information stored within
- If done for profit, up to five years first offense, ten years for subsequent offenses, and/or fine. Otherwise one/fine years or fine
- Exceptions:
  - Owner of service – for any reason
  - For user to access a message from or intended for them



# Providers under the Stored Communications Act

---

- Providers may divulge **content** to recipient or to forward communication
- Providers may not intentionally divulge content of transmission to third parties without
  - Written, intelligent waiver
  - Valid court order/warrant
    - Exc: police may be informed of inadvertent discovery of criminal evidence or reasonable belief of death/physical harm



# Who is a provider?

---

- Maintainer/owner of some system that transmits electronic communication
  - Need not be common carrier (closed Police-only pager system in *Berlach v City of Reno*)
  - Provider employees/agents in normal course of providing service and employment
    - Or to protect users/service in the course of their employment





## Less than interception- Pen Register/Trap and Trace/Customer records

- Pen Register- device to list of all phone numbers, time and duration dialed from one phone
- Trap and Trace-device to list all phones that have dialed one phone number, when and for how long
- Records- Name, dates & times, payment method & addresses (real & IP)
- None may acquire the **contents** of communications



# Pen Register/Trap and Trace restrictions

---


- Providers may use either
  - With informed consent of customer
  - For billing purposes
  - For testing/maintenance/operation of service
  - To protect service, users or connected networks from illegal or abusive acts
  - Under Court wiretap order



# Pen Register/Trap and Trace restrictions

---

- Law enforcement may install/implement PR/T&T
  - As part of legitimate investigation with recipient's permission
  - With valid ex parte order under 18 USC § 3123 (requires neutral finding that information is relevant to ongoing criminal investigation)
  - Remote tapping requirements under CALEA questionable but commercially attractive



# Pen Register/Trap and Trace, continued

---

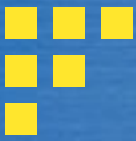
- Not limited to voice/wire
- Could be used to describe sniffer limited to TCP/IP headers
- Could be used by provider without permission of user, if no innocent content is captured



# Civil remedies, as well

---

- Common law tort- intrusion into seclusion (not all states)- damages
- Stored Communications Act- \$1,000 per violation
- ECPA/Wiretap allow civil suits against private parties (damages)
  - No suits against Fed/State for non-Constitutional violations



# Wiretap/SCA interesting cases

---

- Steve Jackson Games v U.S. Secret Service (1995)
  - Interception under Wiretap Act must be contemporaneous (on the wire) with transmission
    - Adopted by most Fed circuits and several states



# Some interesting cases, continued

---

Garrity v John Hancock (2002)

Private employees have no implied expectation of privacy in work email

Muick v Glenayre (2002) Non-government employees generally have no right in work PC contents unless privacy is stated or implied

Konop v Hawaiian Air (2002) Any user can grant access to 3<sup>rd</sup> person and not violate SCA

IAC v Citrin (2006) Unauthorized access to use work laptop to compete with employer while still employed



# Councilman v US (2005)

- Provider offers free email to customers and reads emails (content) from competitors
  - Sends customers competitive offers based upon his reading of email
  - District court dismissed indictment
- Changes rule - interception no longer needs to be contemporaneous with receipt- and not only email!
- Provider protection becomes narrower- interception must be for legitimate business purposes





# What does all this mean?

---

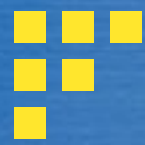
- Providers may intercept some communications to protect themselves, connected networks and their users
- Stored communications have less protection from providers than communications being transmitted
- Councilman is good law only for 1st Circuit- hasn't yet been followed in other circuits



# How to protect yourself?

---

- Get the consent of your users to capture packets, in writing-either in the TOS/AUP or by a separate contract rider
- Get permission from your employer/client, in writing
- Have a sniffer policy- when, how and where and who may use them
- Think about what's sniffing on your network



Questions?

---



# FISA in a nutshell

---

- Exempt from Title III wiretap -18 U.S.C. § 2511(2)(f)
- Creates a special, secret court which may grant an interception order without input from target (50 USC §1801 et seq)
- Interceptions without valid warrant are illegal if under color of law (50 USC § 1809)
  - 5 years imprisonment/\$10k



# FISA in a nutshell, continued

---

- Attorney General/Presidential exception
  - Allows warrantless interception if transmission is between foreign powers & agents thereof
  - No substantial likelihood of intercepting communications of Americans or American companies, & safeguards in place
  - AG must report to Congress 30 days before unless emergency or within 15 days of declaration of war (50 USC § 1802)