

Cybersecurity for Future Presidents

Lecture 2:

How is Data Represented in Computers?

What Laws and Policies control Government searches of communications?

Any Questions?

- About previous lecture?
- About homework?
 - Discuss the debate, briefly
- About reading?

Exercise for next week: data representations, binary material covered last Friday, today, and this Friday

Reading for next week: fundamental policy issues
(show the book)

Note my office hours: Wed. 12-3pm, **442** RH (McDevitt Center Office)

- Please sign up for a "meet the professor slot" if you haven't
- First debaters, I want to meet with at least one team member on each side either today or next week.

Some Recent Events

- Israeli power grid not under attack after all - ransomware aimed at the agency that regulates their power companies
- Report from Harvard's Berkman Center argues "going dark" isn't such a threat after all
- EU and US formulate "safe harbor" policy at the 11th (or 13th!) hour, called "E.U.-U.S. Privacy Shield". Provides a means for EU citizens to complain if their data is misused; apparently includes assurances by ODNI concerning (not doing) "mass surveillance".
- NIST releases second draft of report Recommendation for the Entropy Sources Used for Random Bit Generation

Any from the students?

- Sources (URLs, mailing lists) for some of these events posted on Canvas; join if you are interested

The lecture on one slide

Data Representation and Controlling Government Searches

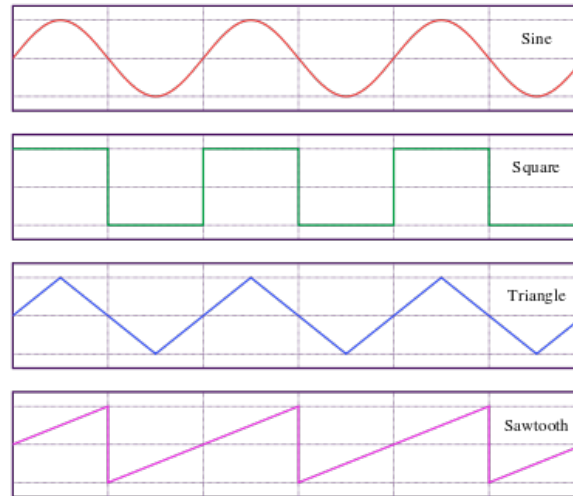
- Technical
 - Analog vs. Digital
 - What is information and what is a bit?
 - How can bits represent different kinds of data?
 - How do phone calls happen?
 - Circuit switching and packet switching
- Policy: Wiretapping and Foreign Intelligence Surveillance
 - Fourth Amendment: searches and seizures
 - Smith v. Maryland
 - Electronic Communications Privacy Act (ECPA)
 - Foreign Intelligence Surveillance Act (FISA)
 - Communications Assistance for Law Enforcement Act (CALEA)
 - Patriot and Freedom Acts

Some cybersecurity issues for a President

- Availability of Communications
 - Especially in case of national emergency
- Protection of sensitive messages
 - Are govt. computers able to protect govt. information?
 - Is my (or my General's, or my Secretary of State's) phone call flowing over communication lines that are within my country, that I can potentially control?
- Surveillance
 - How can I monitor (as authorized) conversations of "bad guys"?
 - Under circuit switching:
 - Identify the circuits used, the endpoint locations are known
 - Under packet switching:
 - Packets may be flowing anywhere. Source address may or may not be reliable
- Other Issues?

Analog vs. Digital

- Analog - continuous
- Digital - discrete
- Digital or analog?
 - Mercury thermometer
 - Light switch
 - Dimmer
 - Vinyl record
 - Compact Disc
 - Voice telephone call
- Why does everything seem to be going digital?
 - Quantification makes it easier to remove noise from digital signals; can recreate clean signal



What is information?

Guessing game



Which shell hides the walnut piece?



Probability of correct guess = $1/2$

What about now?

- Odds of correct guess: 1 in 4
- How many guesses would you need at most?
- What kind of question would you want to ask in order to ask as few questions as possible?



How many yes/no questions to find the prize?



For 8 objects, need 3 questions. Each question gives one bit of information

Eight possibilities

Information from "Is it this one?"

- If "no", you can reject 1 of 8 possibilities
 - If "yes", you can reject 7 of 8 possibilities
- } Unequal information

Information from "Is it in this half of the remaining ones?"

- If "no" you reject 4 of 8
 - If "yes" you reject 4 of 8
- } Equal information

Suppose "no" = 0 and "yes" = 1. Question answers then in effect count the set of objects:

- 000 base 2 = 0 base 10
- 001 base 2 = 1 base 10
- 010 base 2 = 2 base 10
- 011 base 2 = 3 base 10
- 100₂ = 4₁₀
- 101₂ = 5₁₀
- 110₂ = 6₁₀
- 111₂ = 7₁₀

Actually, this is base 8 and is known as "Octal". $7_8 + 1_8 = 10_8$

[Note we are assuming that all positions are equally likely. If there is a bias (e.g., half the time I put the nut under shell number 7), that should change the guesses you would make]

Sixteen possibilities

- If we wanted to count to sixteen in binary, we need another bit - four bits in all
 - 0000 base 2 = 0 base 16
 - 0001 base 2 = 1 base 16
 - 0010 base 2 = 2 base 16
 - 0011 base 2 = 3 base 16
 - 0100₂ = 4₁₆
 - 0101₂ = 5₁₆
 - 0110₂ = 6₁₆
 - 0111₂ = 7₁₆
 - 1000₂ = 8₁₆
 - 1001₂ = 9₁₆
 - 1010₂ = A₁₆
 - 1011₂ = B₁₆
 - 1100₂ = C₁₆
 - 1101₂ = D₁₆
 - 1110₂ = E₁₆
 - 0111₂ = F₁₆
- } Weird but true!
- This is known as hexadecimal (base 16) and is the reason you may see (what seem to be) letters in the midst of memory dumps - you are really looking at base 16 numbers

What is information? How would you measure it?

Reduction in uncertainty (~measure of surprise)

- Whether it might rain (or snow!) this afternoon
- Whether I received a '0' or a '1'

Notice that the reduction in uncertainty when you receive a signal depends on how likely that signal was in the first place. If it was very likely, then receiving it is not much of a surprise. If it was very unlikely, it's a big surprise.

- Term for the randomness of a distribution: Entropy
 - Most random distribution: uniform (hardest to predict next symbol) → maximum entropy.
Examples: coinflip, dice roll

Information Theory

- Branch of mathematics that models information transmission: (Claude Shannon, Bell Labs and MIT, 1940s)
 - How much information can a perfect (noiseless) channel carry?
 - How much information can a noisy channel carry?
- Unit of information: binary digit (=bit) coined by John Tukey, mid 1940s, used by Shannon and others since
- Distinguish: a bit of information vs. a bit of storage

Bits are just numbers, right?

- Yes and no:
 - Numbers can represent
 - Letters: 0000 could be "A", 0001 -> "B" etc.
 - Shades of gray: e.g., 0000 = white and 1111 = black (how many shades of gray does this encoding allow?)
 - Colors: (Red, Green, Blue), intensity of each as a binary number
 - Sounds: sound wave is acoustic pressure; quantify the pressure as a binary number, sound becomes a sequence of numbers (hence Compact Discs vs vinyl records)
 - Machine instructions: the elements of computer programs are machine instructions that are interpreted by the computer's Central Processing Unit
 - Note that if you want to convert the numbers back into colors or sounds, you need a transducer - a printer, display screen, or speaker that can convert the numbers back into the physical dimension

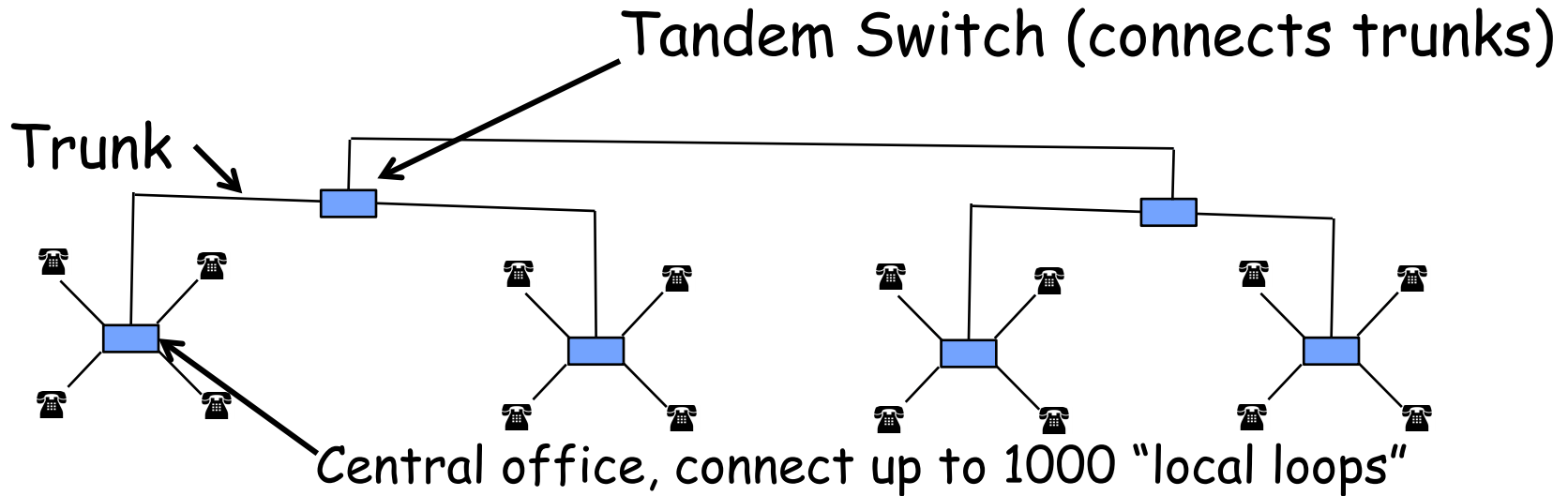
A Little History of Telephony in the U.S.

- 1876: Alexander Graham Bell patents telephone
 - AT&T develops telephone systems
 - Central switching offices (manual)
- 1891 Strowger switch patented (first automatic switching, "step by step")
- 1925: Bell Laboratories created from engineering departments
 - Automatic switching equipment developed
 - National communications networks, including hardening for national security
- 1940s: WWII stimulates voice encryption work "SIGSALY"
 - Mobile phone network of hexagonal cells proposed
- 1950s: Transistors and laser technologies invented
- 1960s: Wireless and cellular phones invented, No. 1 ESS 1965
- 1970s: packet switching research
 - 1973: First consumer equipment cellular phone call
- 1980s: rise of (D)ARPANET
- 1990s: NSFNET, commercial Internet, WWW
- 2000s: digital convergence, VoIP, streaming, Skype, ...

Architecture of the traditional Public Switched Telecommunications Network (PSTN) or Plain Old Telephone Service (POTS)

- Circuit Switched: Effectively creates a dedicated wire path between caller and callee, as follows:
 - customer requests connection by dialing a number;
 - switching equipment locates a path to the requested number
 - May traverse various trunks depending on load and availability
 - Ring initiated at called number
 - Callee answers and physical path (in effect, a dedicated wire) is established between the two telephone
 - Voice (or other) traffic is transmitted over the path
- Details are actually more complicated -- discuss
- Note the distinction between the traffic and the facilities used to transmit the traffic - these are in effect different networks

How telephones used to work



- Circuit switching:

- Create a wire path between two telephone instruments
- Hierarchical switching network
- Amplifiers to regenerate signals en route

Wiretapping a circuit-switched line

- Find a point anywhere on the path of the circuit (usually at central office)
 - Splice into the circuit
 - Record the traffic
- "Pen Register": record of which two telephones were connected, when, and for how long (e.g. for accounting purposes)

How telephones work today

- Voice signal digitized at endpoint and broken into packets (fixed size blocks of bits)
- Address of destination attached to packet
- Packet sent into packet-switching network; different packets may take different paths through the network

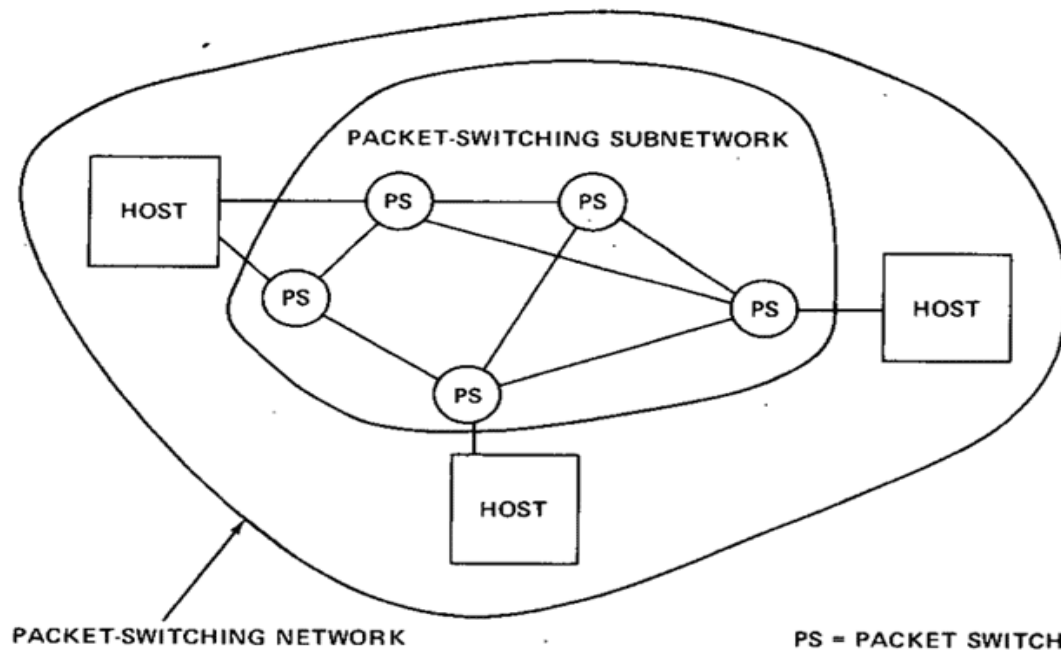
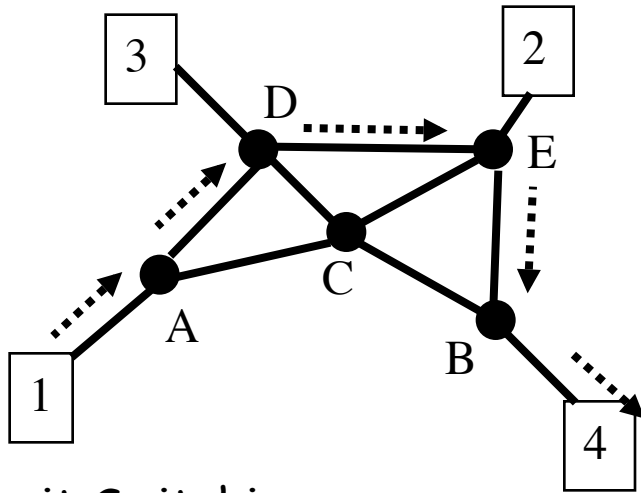


Fig. 1. Typical packet switching network.

From: <http://www.internethalloffame.org/internet-history/timeline>

Allocating network resources: Circuit Switching vs. Packet Switching



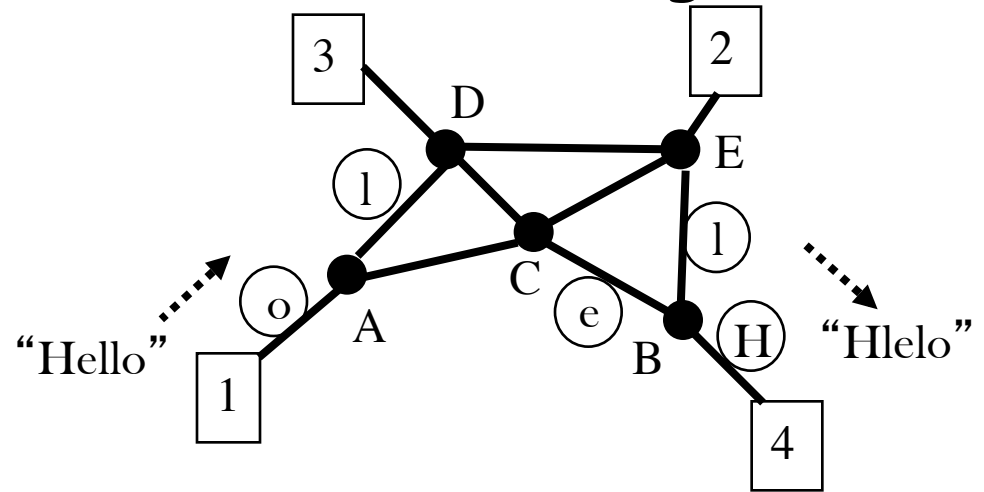
Circuit Switching:

- Call request
- Reserve dedicated “circuit” in net
- Transfer information
- Disconnect circuit

Low, constant delay in operation

Traffic follows one path

Potential waste of
idle allocated bandwidth



Packet Switching :

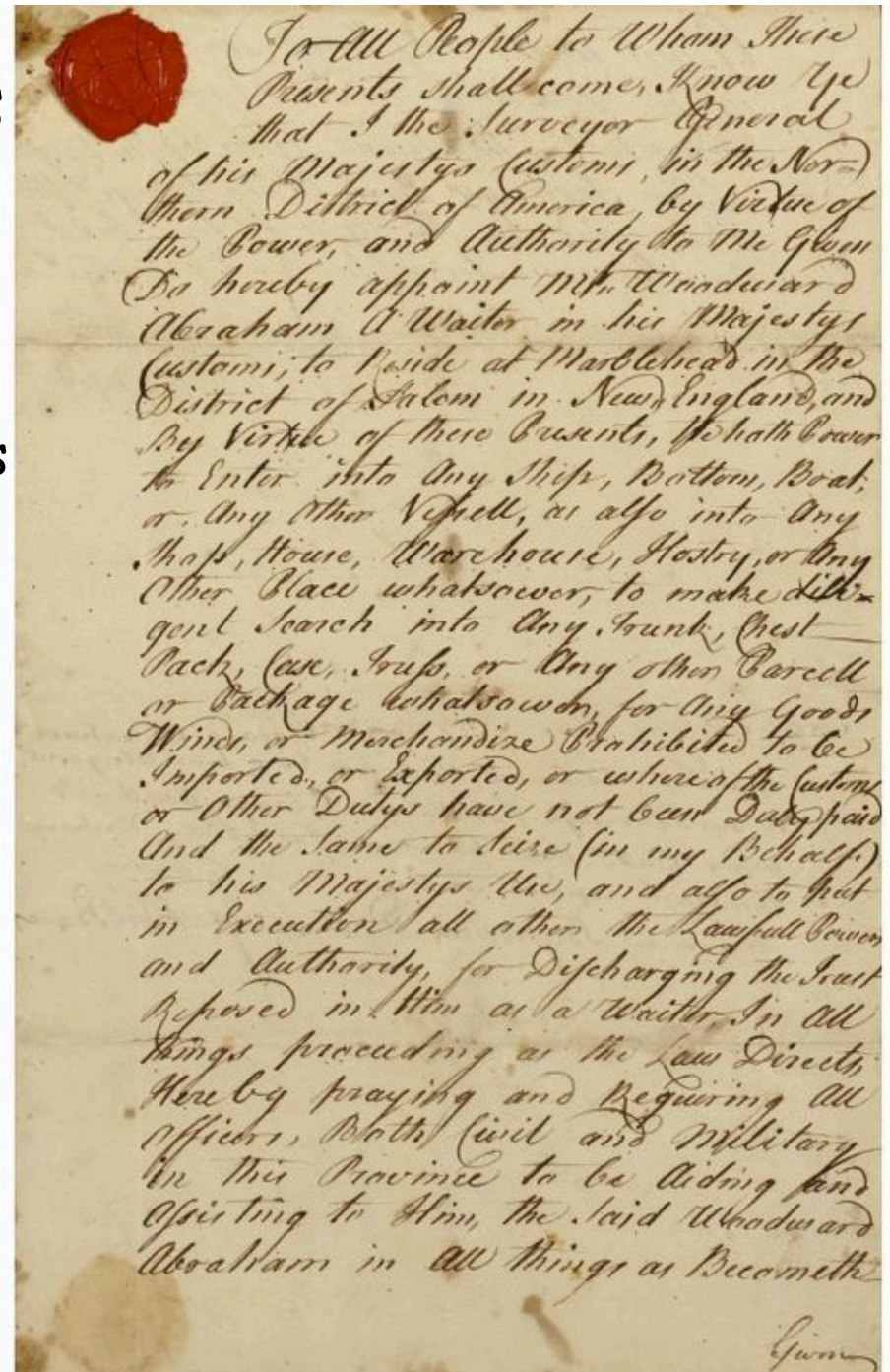
- Message chopped into packets
 - Each node forwards packet towards destination, (dynamic routing, best effort)
 - Destination reassembles, re-orders, delivers to host
 - Deliver message to recipient
- No call setup; more flexible resource use
Traffic may follow many paths, arrive out of order
“Stateless” network

Wiretapping a packet-switched phone call

- Need a way to collect all of the packets and reassemble them
- What if it's a cellphone you want to monitor? May enter the network from many different endpoints
 - But cellphones identify themselves to the network and also provide valuable location data
- Wiretapping may mean monitoring all the packets and just selecting those that satisfy legal warrant

Writs of Assistance, 1760s

- Smuggling was common in British American colonies in this period
- Crown issued "writs of assistance" that authorized customs inspectors to search nearly anything (ship, property, household) without any further justification
- Widely unpopular and fueled the Revolutionary War
- This is an image of one such writ →



To All People to Whom These
Parents shall come, Know Ye
that I the Surveyor General
of his Majestys Customs, in the Nor-
thern District of America, by Virtue of
the Power, and Authority do Me Given
do hereby appoint Mr. Woodward
Abraham & Waiter in his Majestys
Customs, to reside at Marblehead in the
District of Salem in New England, and
by Virtue of these Parents, do hath Power
to Enter into any Ship, Bottom, Boat,
or any other Vessel, or also into any
Shop, House, Warehouse, Store, or any
other Place whatsoever, to make dili-
gent Search into any Trunk, Chest,
Pack, Case, Truss, or any other Parcel
or Package whatsoever, for any Goods
Wines, or Merchandise Prohibited to be
Imported, or Exported, or whereof the Customs
or other Dutys have not been duly paid
And the same to Seize (in my behalf)
to his Majestys Use, and also to put
in Execution all other the Lawfull Powers
and Authority, for Discharging the Trust
Reposed in him as a Writter. In all
things proceeding as the Law Directs
Hereby praying and requiring all
Officers, both Civil and Military
in this Province to be aiding and
Assisting to him, the said Woodward
Abraham in all things as Becometh

Given

Text of a Writ of Assistance, 1762

"To All People to Whom These Presents shall come, Know Ye that I the Surveyor General of his Majestys Customs, in the Northern District of America, by Virtue of the Power, and Authority to Me Given Do hereby appoint Mr. Woodward Abraham A Waiter in his Majestys Customs, to Reside at Marblehead in the district of Salem in New-England, and
By Virtue of these Presents, He hath Power to Enter into Any Ship, Bottom, Boat, or Any Other Vessell, as also into Any Shop, House, Warehouse, Hostry, or Any Other Place whatsoever, to make diligent Search into Any Trunk, Chest, Pack, Case, Truss, or Any other Parcell or Package whatsoever, for Any Goods, Wines, or Merchandize Prohibited to be Imported, or Exported, or whereof the Customs or Other Dutys have not been Duly paid and the Same to Seize (in my Behalf) to his Majestys Use,

and also to put in Execution all other [of] the Lawfull Powers and Authority for Discharging the Trust Reposed in Him as a Waiter, In All things proceeding as the Law Directs, Hereby praying and Requiring All Officers, Both Civil and Military in the Province to be Aiding and Assisting to Him, the Said Woodward Abraham in all things as Becometh."

Bill of Rights, Fourth Amendment, 1791

What:

- 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.

Notice:

- "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"
- "no warrants shall issue, but upon probable cause"
- Long before the telegraph, telephone, computer
- Information was manifested on paper, parchment, etc.
- How would you interpret this for modern technology?
- What questions are important?
 - 3 minutes to confer
 - Discuss

Some questions to consider

- In the context of modern criminal investigation involving computers and telecommunications,
 - What might be searched?
 - What might be seized?
 - How might a warrant be framed so as to be "particularly describing the place to be searched, and the persons or things to be seized. "

Charles Katz v. U.S., 1967

- Katz was a Los Angeles gambler who placed bets using a public pay phone
- Police installed a listening device on the outside of the phone booth, without a warrant, and evidence collected was used to convict him
- Supreme Court held that "the Fourth Amendment protects people, not places"
 - By entering phone booth, Katz had a legitimate expectation of privacy of his utterances
 - Even though no trespass (an issue in placing microphones in houses, for example) was involved, this was deemed an improper unwarranted search. A warrant would have made it OK

Smith v. Maryland, 1978, Call Data Records (pen register)

What happened:

- Phone company, at police request, but without a warrant, installed a pen register at central office to collect Smith's call records
- The call records, with other evidence, were used to obtain a search warrant, and Smith was convicted
- Smith appealed on the basis that the search of the pen register lacked a warrant

Decision:

- The Supreme Court held that no warrant was required because the caller had no expectation of privacy for the phone numbers called, since this information is freely provided to the phone company and constitutes a business record
- Hence it is permissible for the phone company to provide this information to the police without a warrant

Electronic Communications Privacy Act, 1986

- Responding to advances in technology, including Signaling System 7 (SS7); telephone switch that made it easier to collect CDRs
- Distinguishes:
 - Wire communications: carrying human speech over wire, cable, or cellphone
 - Oral: by sound waves over the air
 - Electronic: any electronic communication not wire or oral includes email, fax
- Easily intercepted (e.g., unencrypted) radio communications protected from eavesdropping
- Only a court order, not a warrant, needed for "probable cause" demonstration required.
- Stored electronic communications: private communications prohibited; gov't interception requires search warrant; mail stored for 180 days or less. Contents stored for less than 180 days after having been read are less protected.
- Also authorized "roving" wiretaps

Lecture really ended about here – will cover this and remaining slides in next lecture

Communications Assistance for Law Enforcement Act (CALEA) 1994

- Law enforcement not satisfied with ECPA and wanting better assistance for wiretaps
- CALEA required telecomm carriers to
 - design systems to quickly isolate call content, as well as origin/destination phone numbers
 - Provide this info to LE in a format and at a location of LE's choosing
- Funding provided to telecom suppliers to accomplish this
- Idea was to preserve government wiretap access in new environment, not to expand it
- FCC charged with overseeing implementation
- Controversial; took years to implement
- Extended to Internet and Voice of IP (VOIP), 2005

Surveillance for law enforcement vs surveillance for foreign intelligence

- What differences might there be in surveillance for these different purposes?
 - Take 3 minutes to consider: aims, scope
 - Discuss

Foreign Intelligence Surveillance Act, 1978

- Historically, President claimed authority for electronic surveillance for non-criminal, national security purposes (i.e., spying).
- Abuses uncovered by Congress in 1975 prompted the passage of the Foreign Intelligence Surveillance Act (FISA) of 1978 as a means of authorizing and controlling such surveillance through warrants
- FISA established that non-criminal electronic surveillances within the United States were only permissible for the purpose of collecting foreign intelligence and/or foreign counterintelligence.
- FISA set up a court (FISC) whose members were public but whose proceedings were secret to authorize (or not) such surveillances proposed by intelligence organizations
- FISA allowed warrantless wiretapping of communications outside the US and also communications terminating in the US if at least one party was outside the country (and this wasn't being used as a dodge to target a U.S. person)

USA PATRIOT Act, 2001

- In the wake of 9/11 attacks, this act lowered the barriers between surveillance for national security / counterintelligence and law enforcement
- Section 215 of the act enabled collection of "business records" for national intelligence purposes without a warrant.
 - This was thought to enable collection of individuals library records
 - It was used to justify NSA's massive collection of CDRs from US telephone networks.
 - Legality of this collection, when it was made public, became a significant matter of public debate and legal challenge
 - Revisions to the Act in 2015

FISA Amendments Act, 2008

- Warrantless wiretapping program, initiated following 9/11 attacks, was revealed by New York Times in late 2005; reportedly discontinued January 2007
 - Substantial doubts raised as to whether the program was legal under existing laws
- FISA Amendments Act of 2008
 - Added a Title VII, including Section 702
 - Authorizes Attorney General and Director of National Intelligence jointly to authorize targeting of individuals (non U.S. Persons) reasonably believed to be outside of the U.S.
 - Authorized the PRISM program of which you may have heard, and some others

USA Freedom Act, 2015

- June, 2013 Edward Snowden began releasing large volumes of classified data on NSA and GCHQ surveillance programs, evoking substantial public reaction, still ongoing
- In particular, program to collect "meta-data" - CDRs of all U.S. phone calls challenged as illegal (litigation still ongoing)
- Pres. Obama agreed to limit this program by having the telephone companies, rather than the government, hold this data, with the government allowed to query it under supervision
- These limitations are incorporated in authorization of the program passed in the USA Freedom Act last June