Government Surveillance

Professor Grimmelmann
Internet Law
Fall 2007
Class 12

Where we are

- Introduction
- Part I: Public Law
  - Jurisdiction
  - Free Speech
  - Intermediaries
  - Privacy
- Part II: Private Law

Road map

What kind of data?

Content

To whom?

Government

Private parties

Non-content

Last Tuesday

Today

Next Tuesday

In today's class

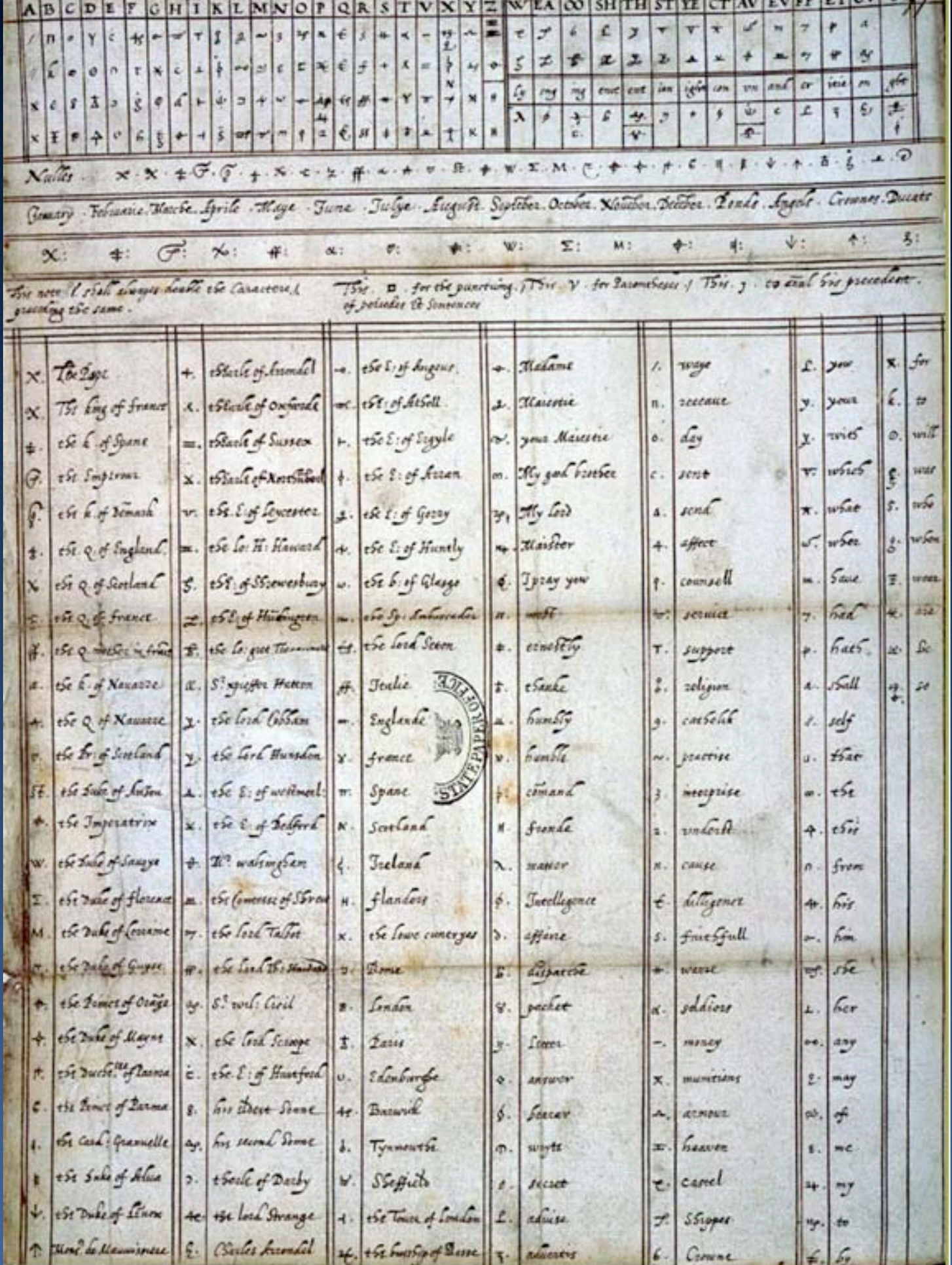
- The crypto wars
- Digital criminal procedure
  - Fourth Amendment
  - ECPA
- The national surveillance state

A reminder re: ECPA

- You. Can. Read.
  - The statutes are complex and changing
  - This isn't a a crim pro course
  - In practice, you'll look it up
- Today, we're focusing on *controversies* rather than on statutory details
- For more details, go read Kerr's casebook

Dszqtuphrsbdiz

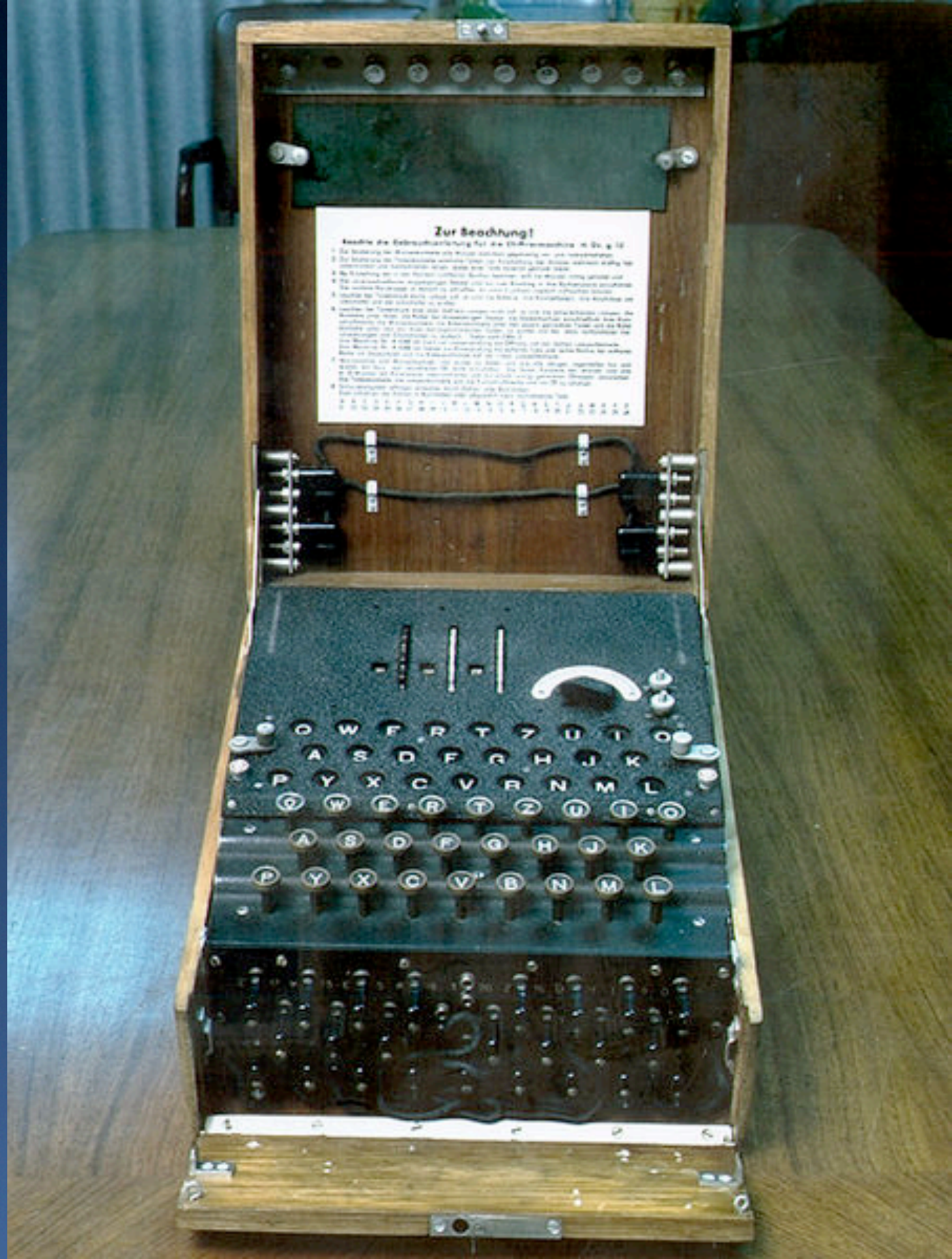
ca. 350 B.C.: Scytale

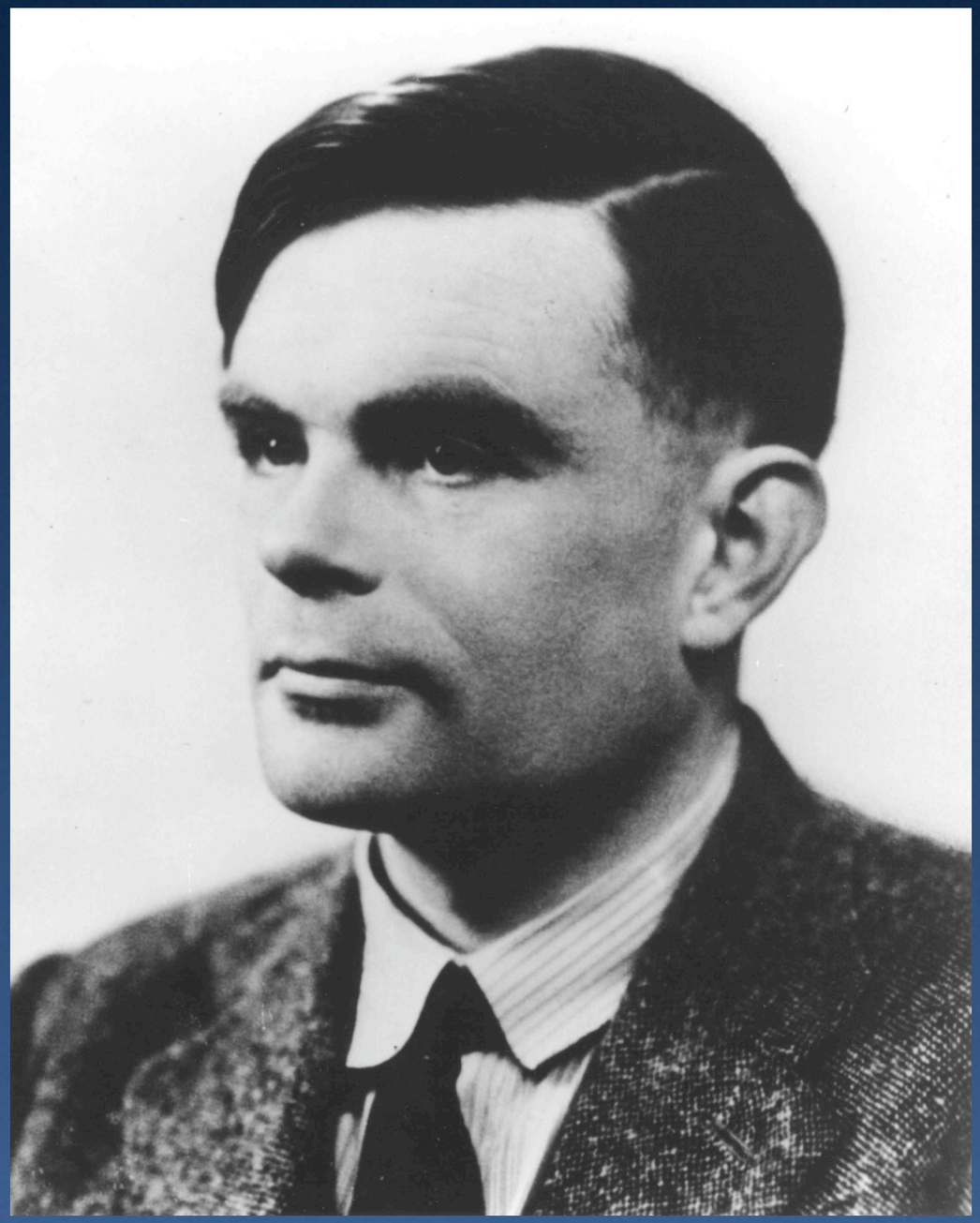


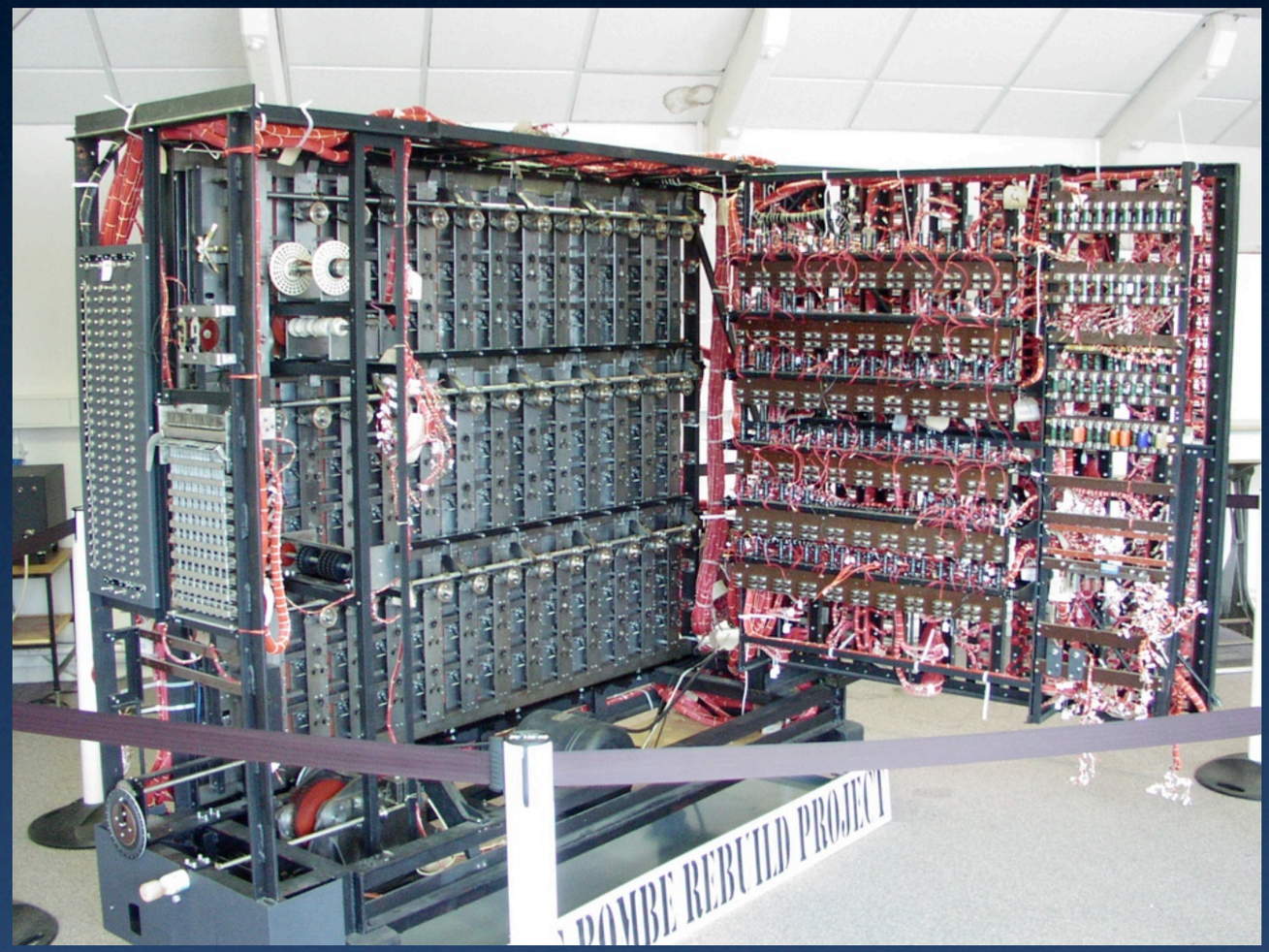
1586: Mary Queen of Scots's ciphers . . .

. . .and her execution

WWII: The German Enigma machine . . .





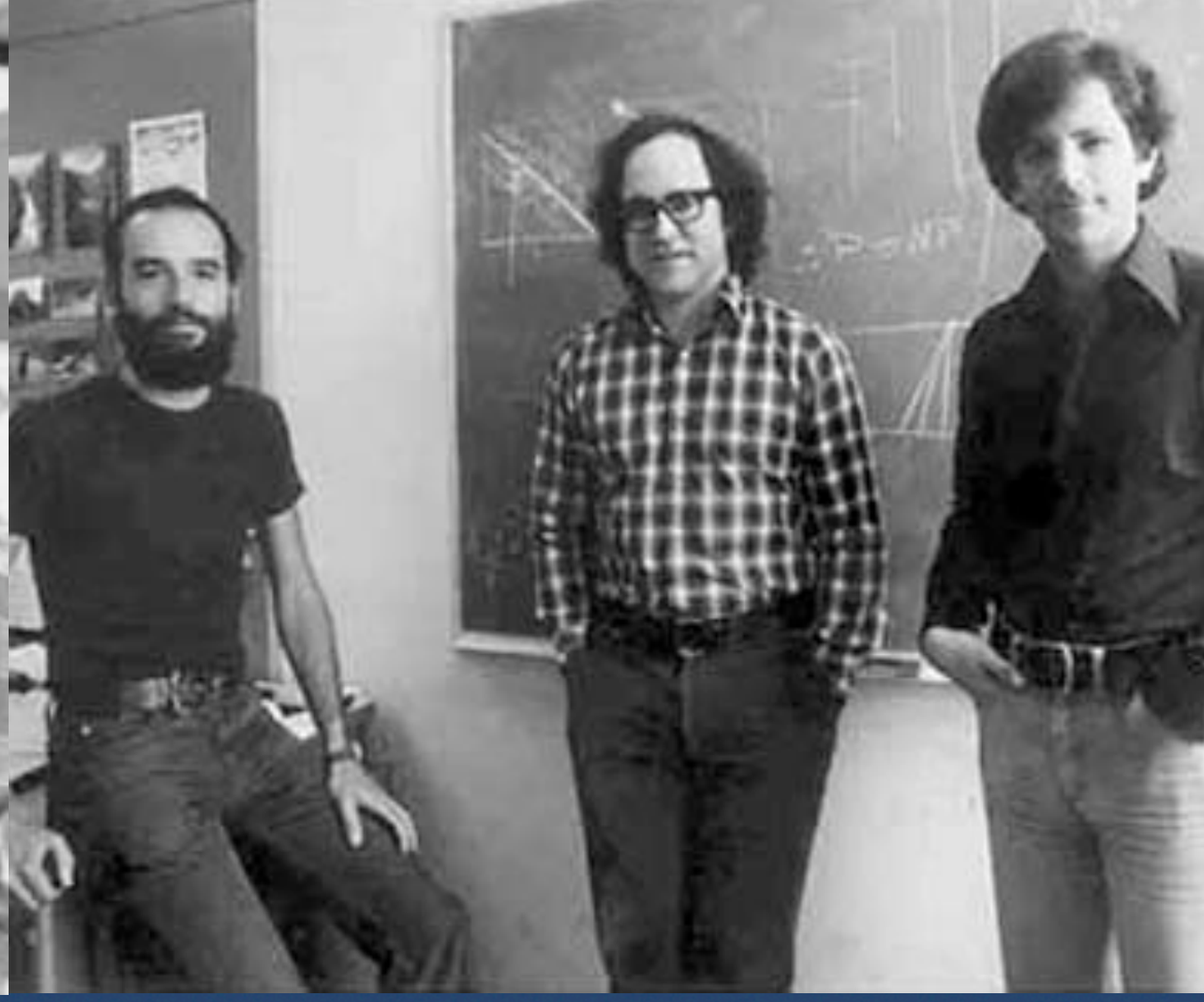


. . . and the Turing-designed machine that could decode it

What's crypto got to do with it?

- Governments have competed for centuries on the strength of their cryptography
- Bad cryptography costs lives
- Cryptography is a form of self-help against government surveillance
- And cryptography always involves cutting-edge computational technology

1976:
Diffie,
Hellman,
& Merkle



1977:
Rivest,
Shamir,
& Adelman

The inventors of public-key cryptography

Public-key crypto is heady stuff

- Alice can send Bob a message such that:
  - No one but Alice can read it
  - No one but Bob could have sent it
  - Alice and Bob don't know each other
  - No one else can learn who they are

Who likes crypto?

- Nerds
- Criminals
- Utopian anarchists
- And major multinational corporations
  - People want privacy
  - And crypto has many other uses (digial signatures, authentication, error-correction, watermarking, DRM, etc.)

No Such Agency

The NSA wakes up

- The NSA used to supervise most crypto
  - But now, the research was out there
  - And companies wanted to ship crypto
- After a decade of fumbling, the NSA moves on two fronts:
  - Standardize crypto in ways they like
  - Prohibit exporting it to the bad guys

Weak codes and key escrow

- 1976: NSA suspected of adding a backdoor to the Data Encryption Standard
- 1992: AT&T triggers controversy with a plan to sell crypto-enabled phones
- The feds propose the Clipper Chip, which would hardwire key escrow into phones
- Controversy rages

The death of the Clipper Chip

Matt Blaze

It turns out that Clipper is easy to fool, making the escrowed key useless, and pretty much killing off key escrow schemes

Bernstein v. United States

- At stake: can Daniel Bernstein publish his crypto research on the Internet?
- Why would that be an "export?"
- The rule would be obviously absurd if he were a historian or an economist
- *Held*: code is speech
  - Does this mean that software is exempt from government regulations?

Bernstein's legacy

- *Cause célèbre* for programmers, for whom the export controls were tantamount to the government telling them how to do their jobs
  - Cf. the ethical commitment to sharing information and knowledge
- Code is speech, for what that's worth
- The export restrictions still exist, but have been enormously loosened

Criminal Procedure

“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.”

Fourth Amendment refresher

- A warrant is the gold standard
  - It makes any properly-done search OK
  - It requires probable cause
  - There are also procedural rules (neutral magistrate, oath or affirmation, particularity)
- If there's no warrant, the evidence is excluded

Warrantless searches

- Some searches are "reasonable" even without a warrant
  - E.g. consent
  - E.g. exigent circumstances
- And some things aren't even "searches"
  - The Fourth Amendment doesn't apply unless there's a "reasonable expectation of privacy"

United States v. Charbonneau

- "Charbyq" goes into "BOYS" and "PRETEEN" chatrooms and sends child pornography to an FBI agent
  - The agent gets a search warrant and learns Charbonneau's name from his ISP
- Sanity check: If there was a search warrant, why is this case even in court?
  - Charbonneau is trying to suppress the evidence on which the warrant was *based*

This is not a hard case

- If you hand child pornography to an FBI agent, do you have a reasonable expectation of privacy?
  - If you mail it to him?
  - If you email it to him?
- No, no, and no
- You took the risk you might be dealing with an FBI agent

United States v. Hambrick

- "blowuinva" propositions "Rory14" in a chat room named "Gay dads 4 sex"
  - Rory14 is actually a cop, who gets a state subpoena to learn blowuinva's name
  - But the subpoena is invalid, because it was signed by another cop
- The government learned Hambrick's name improperly. Why doesn't that end the case?

The Fourth Amendment analysis

- There's no Fourth Amendment issue if the government's actions don't violate your reasonable expectation of privacy
- There's no reasonable expectation of privacy in the (noncontent) information you expose to your ISP
- Explanation: lots of people at the ISP have access to that information, and who knows what they might do with it?

Quick quiz

- *Charbonneau* involved what sort of information? Content or non-content?
  - Content
- And to whom was it revealed?
  - Other users
- In *Hambrick*: what kind, and to whom?
  - Non-content, and to the ISP

And now, the punch line

- Title II of ECPA allows the government to acquire stored communications (i.e. content) (e.g. emails) from ISPs and other intermediaries with just a court order, rather than a warrant
- Is that constitutional?
  - Use *Charbonneau* and *Hambrick*
  - Use policy arguments

There is no settled answer

- *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007) held that the SCA's court-order provision is unconstitutional
  - There's a pending motion for rehearing
  - With high-powered amicus briefs on both sides
- We live in exciting times

ECPA Again

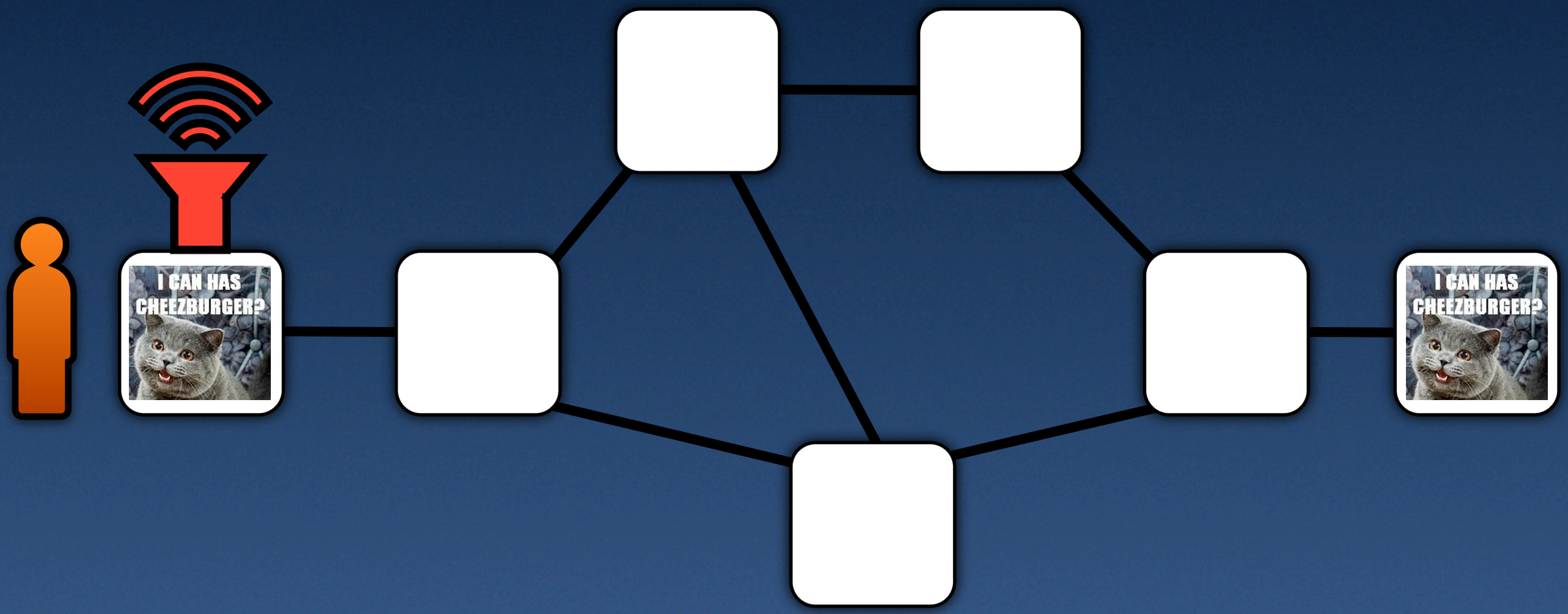
Steve Jackson Games

- The Secret Service is investigating the copying of some phone company manuals
  - Which might not even be a crime
    - They find a copy of the file on a BBS run by Blankenship, who works for SJG and wrote the manual for GURPS Cyberpunk
- The Secret Service mistakes this for *actual* hacking instructions and raids the company, taking a computer with emails

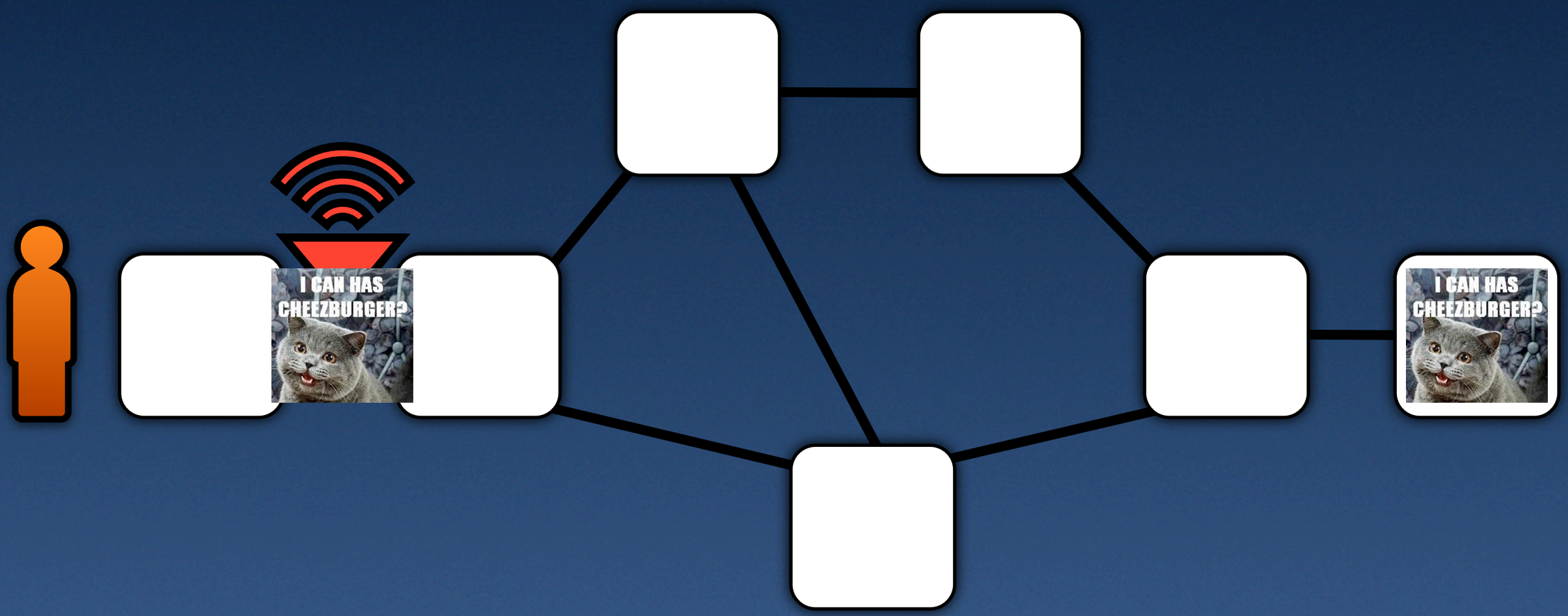
Did the government "intercept?"

- The question matters because interception violations have damage remedies
- *Turk* had held that taking an audiotape of a prior conversation isn't a seizure because it's not simultaneous with the conversation
- Does this analogy work?
- Does it lead to a sensible technical rule?

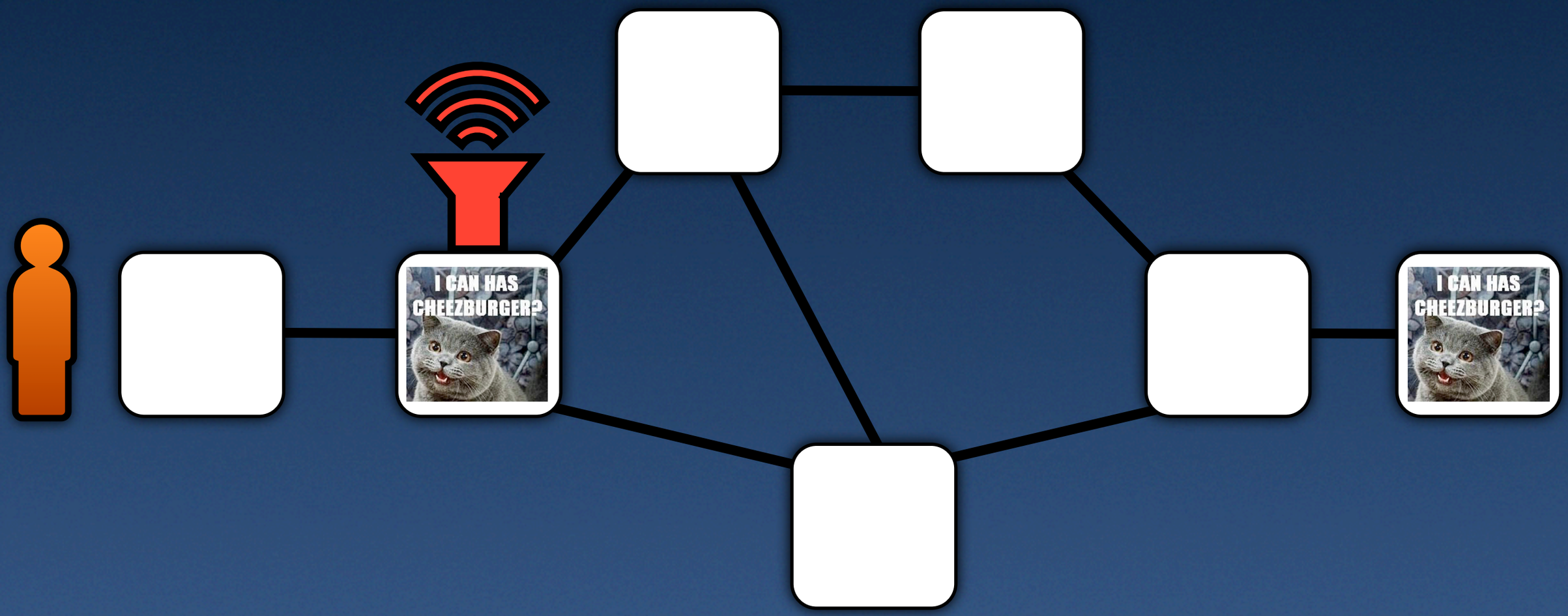
What happened in *Steve Jackson*



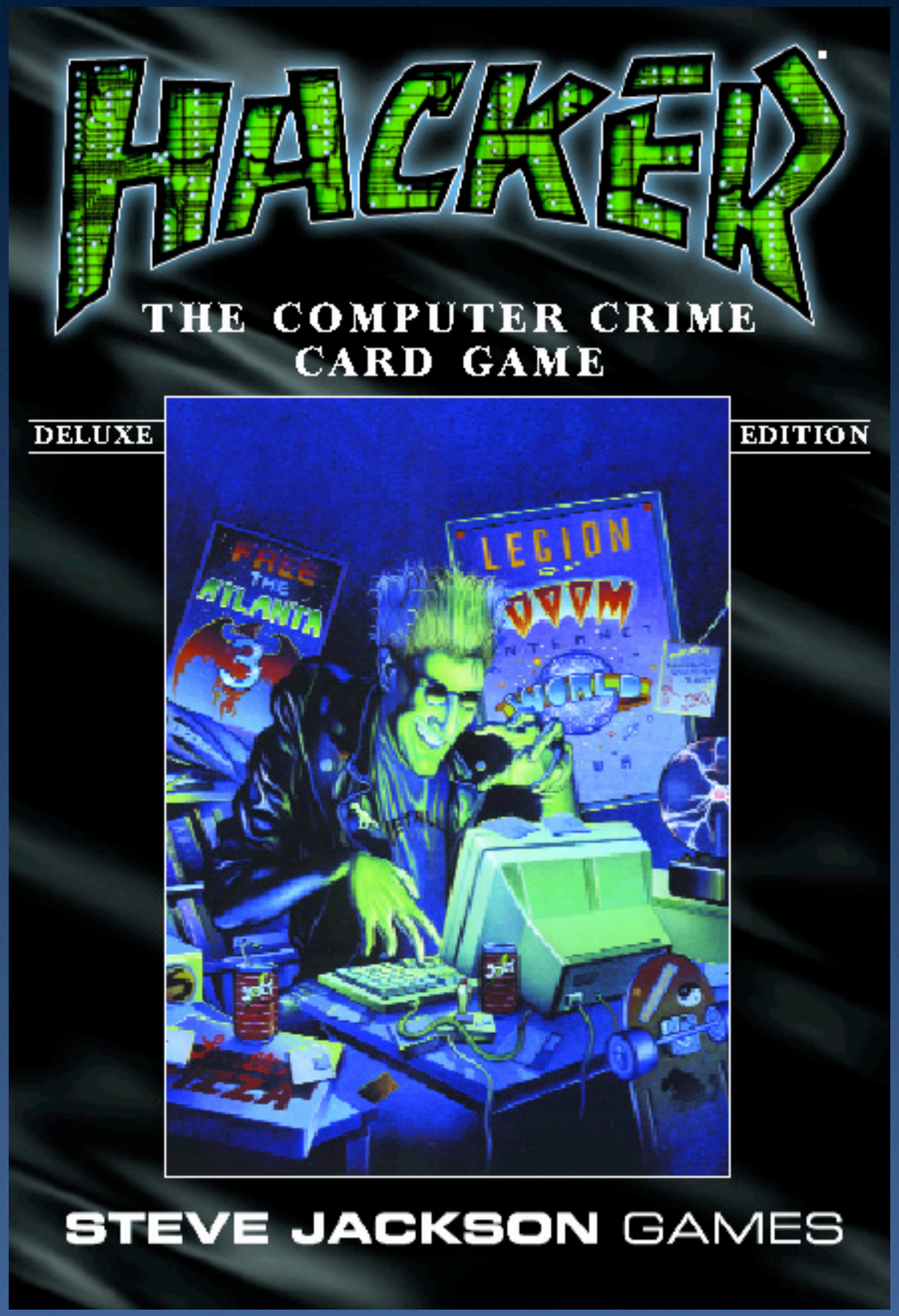
“Interception” according to the court



No “interception?”



The last laugh



ECPA and content acquisition

- Prospective: Title I (Wiretap Act), 18 U.S.C. §§ 2510 *et seq.* ("Interception")
- Retrospective: Title II (SCA), 18 U.S.C. §§ 2701 *et seq.* ("electronic storage" and "remote computing service")
  - NB: This is the same chapter that deals with disclosing non-content subscriber records

Pervasive surveillance

FISA (1978)

- Foreign Intelligence Surveillance Act
  - The Attorney General may engage in secret surveillance of "foreign powers" and their agents without a court order
  - But must make a sealed certification to a classified court "immediately"
- There are procedures for using the evidence so gathered in criminal proceedings

CALEA (1994)

- Communications Assistance for Law Enforcement Act
- Wiretaps don't just grow on trees
- The phone company has to make its equipment wiretap-ready
  - So do ISPs
  - And "interconnected" VoIP services
  - And?

Carnivore (ca. 1997)

- Worst-named FBI program in history
  - Omnivore recorded all traffic through an IP switch; Carnivore is supposed to record only the "meat"
  - Not an easy technical problem
- And really, how else would you "listen in" on IP traffic on the Internet?
- Big concerns: minimization and oversight

Total Information Awareness (2002)

- Data mining on steroids
- Most Orwellian logo ever
- Defunded by Congress
- Parts of it live on

Echelon

- The NSA intercepts international telecommunications
- Details on what they do with the data are few and far between

Terrorist Surveillance Program

- Details were tightly controlled, but . . .
  - Some kind of wiretapping of a form that FISA didn't authorize
  - The administration argued that the AUMF provided legal authority
- After losing Congress, the Administration brought the TSP under FISC control
  - But it continues . . .

NSA call database (2001)

- It's a gigantic pen register system
  - Call-detail records for *trillions* of calls, obtained with cooperation of telcos
  - Data-mining on steroids again
- Note: no individualized court orders
  - That's a prima facie violation of ECPA
  - The EFF is suing AT&T

Government surveillance programs

- FISA
- CALEA
- Carnivore
- Total Information Awareness
- Echelon
- NSA call database
- Terrorist Surveillance Program

Should we have listened to the cypherpunks?

Next time

"You have no privacy. Get over it."