

## Privacy from Government

## Fourth Amendment

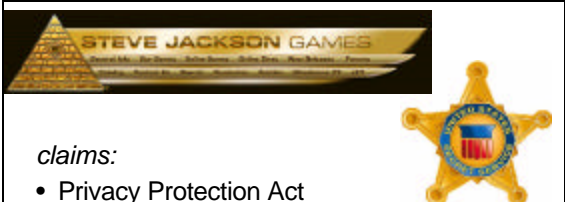
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the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

- Which of these is an email most like?



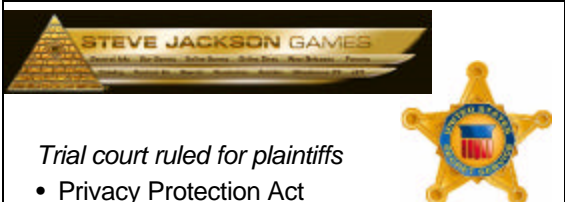
- Which of these is an email most like?
  - Unless encrypted, it travels through the ‘Net like a postcard, visible to anyone stationed at any of the ISP “hops” along its route
  - If most people don’t realize this, is their “expectation of privacy” reasonable?
  - Should we give more protection than the Fourth Amendment requires?

- ### Statutory Protections, and their limits
- Wiretap Act (Omnibus Crime Control and Safe Streets Act of 1968)
  - Electronic Communications Privacy Act (ECPA) of 1986
    - Wiretap Act, updated
    - Stored Communications Privacy Act
    - Pen Register / Trap and Trace
  - USA PATRIOT Act, 2001



*claims:*

- Privacy Protection Act
- Wiretap Act (ECPA Title I)
- Stored Communications Act (ECPA Title II)



*Trial court ruled for plaintiffs*

- Privacy Protection Act
- Stored Communications Act (ECPA Title II)

*On appeal:*

- Wiretap Act (ECPA Title I)
  - Interception?

<i>requests</i>	Real-time acquisition	Historical information
Contents of communications	Wiretap Act (super-warrant) or consent	Unopened: Warrant
		Opened: Subpoena with notice (poss. delayed)
Non-content-transactional or subscriber information	Pen register / trap-and-trace order (warrant-minus) or consent	Subscriber info: subpoena
		Transactional: 2703(d) “specific and articulable facts” order

*Adapted from Mark Eckenwiler*

### NSLs

§ 2709. Counterintelligence access to telephone toll and transactional records

**(a) Duty to Provide.**— A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

**(b) Required Certification.**— The Director of the Federal Bureau of Investigation, or his designee... may

... (2) request the name, address, and length of service of a person or entity if the Director ...certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is **relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities**, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

**(c) Prohibition of Certain Disclosure.**— No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

## USA PATRIOT Act

- PATRIOT changed standard for obtaining administrative subpoena
  - *from* “specific and articulable facts giving reason to believe that the person ...[was] a foreign power or agent of a foreign power”
  - *to* “certification ... that information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities”

## *Doe* argues

- Violation of *Doe*'s rights
  - Fifth Amendment due process
  - Fourth Amendment search
- Violation of *Doe*'s *subscribers'* rights
  - First Amendment right to anonymous speech
  - “transactional records” might include content, association
- Violation of *Doe*'s First Amendment rights
  - First Amendment right to discuss process
  - “categorical, perpetual, and automatic ban on disclosure”

## You're the Fed

- As a government lawyer, you're involved in a criminal investigation. Can you get the information? With what tool? What showing do you need?
  - The email addresses of a suspect's correspondents
  - The contents of a suspect's past emails to BigRed, a suspected co-conspirator
  - The time and date of the suspect's last ten Internet connections through ISP
  - The name of the Internet user BigRed@hotmail.com
  - Future emails the suspect might send to BigRed
  - Immediate alerts when the suspect logs on to ISP in the future