

# Privacy

## Chapter 13



## The 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."

3

## Kyllo v. United States

- Thermal imaging reveals unusual amount of heat radiating from Danny Lee Kyllo's garage.
- Search warrant reveals over 100 marijuana plants growing in Kyllo's home.
- Ninth Circuit Court upholds conviction.
- Supreme Court overturns conviction ruling that thermal imaging constituted a search.

4

## "The Right To Privacy"

- "The narrower doctrine may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that **modern devices** afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation." [emphasis added]

*The Right to Privacy*  
Samuel Warren and Louis Brandeis  
Harvard Law Review, 1890

5

## Questions

- What does privacy mean?
  - The "right to be left alone"? What does that mean?
- Do we have a right to privacy?
  - If I see you at a street corner, can I sell that information (provided there is a buyer)?
  - What if you buy something at my store?
    - How many of you have a shopping club card?

6

## Cookie

- **cookie:** parcels of text sent by a server to web browser and then sent back unchanged by the client each time it accesses that server
  - Used to remember the user who is visiting the website in order to show the appropriate content.
  - Responsible for "Remember Me" checkbox.
- Options:
  - Never accept cookies
    - Not really an option: Many legitimate websites require cookies to function
  - Ask each time a server wants to set a cookie
    - Would be very annoying, so also not really an option
  - Accept all cookies
    - No other option?
    - Browser lets you choose to delete cookies when you close your browser.

7

## Whose Information Is It?

- If you buy something at a store, what can the store do with your information?
  - No Uses: Delete information after transaction.
  - Opt-in: Can use if you approve the use.
  - Opt-Out: Can use unless you object.
  - No Limits: Store owns the information.
  - Internal Use: Can use to conduct business with you, but nothing else.

8

## Facebook

- Terms of Use
  - <http://www.facebook.com/terms.php>
- "We reserve the right, at our sole discretion, to change, modify, add, or delete portions of these Terms of Use at any time without further notice. If we do this, we will post the changes to these Terms of Use on this page and will indicate at the top of this page the date these terms were last revised. Your continued use of the Service or the Site after any such changes constitutes your acceptance of the new Terms of Use."

9

## Facebook Privacy Change Upoar

- "By posting User Content to any part of the Site, you automatically grant, and you represent and warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose, commercial, advertising, or otherwise, on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing. *You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.*"
- Changed February 4, 2009. Italicized sentences were deleted. Discovered February 15, 2009. Put back February 16, 2009.

10

## What Does Your Search Say About You?

- August 4, 2006: AOL releases search data from a 3-month period for 650,000 users
- Users were not personally identifiable—identified by a unique key.
  - Search history of individuals could be compiled.
  - Some people were identified by what they searched.
- August 21, 2006: AOL's CTO resigns.

11

## Clartext

- **clartext:** form of a message or data which is in a form that is immediately comprehensible to a human being without additional processing
- Most e-mails are sent in the clear.

12

## Cryptography

- Private-key cryptography
  - Single key to encrypt and decrypt messages
  - Sender and receiver share the same key
- Public-key cryptography
  - Most famous algorithm is RSA

13

## RSA

- Algorithm for public-key cryptography invented in 1977
- Named after Ron Rivest, Adi Shamir, and Leonard Adleman at MIT
- Independently invented by British intelligence four years earlier in 1973 (information was classified until 1997)

14

## Public-Key Cryptography

- Two keys: public key and private key
  - Public key encrypts messages
  - Private key decrypts messages
- Receiver generates both keys and publicizes public key
- "Impossible" to determine private key from public key

15

## PGP: "Pretty Good Privacy"

- Software that provides cryptographic privacy and authentication.
  - Created by Phil Zimmermann in 1991
- Uses keys with at least 128 bits
  - Keys larger than 40 bits were considered munitions within the definition of the US export regulations before 1996
  - Zimmerman published entire source code in a book (export of books are protected by the First Amendment)

16

## United States v. Boucher

- December 17, 2006: Sebastien Boucher crosses border from Canada to USA at Derby Line, Vermont.
- Laptop was inspected. Boucher questioned.
- Child pornography was found on the laptop.
- Laptop was seized and powered-down.
- December 29, 2006: Laptop was booted. Contents were inaccessible due to PGP encryption.
- Boucher refuses to divulge the PGP key.
- November 29, 2007: Magistrate opines "Compelling Boucher to enter the password forces him to produce evidence that could be used to incriminate him." (Fifth Amendment)
- January 2, 2008: United States appeals magistrate's opinion.
- February 19, 2009: Judge reverses magistrate's opinion.

17

## Resources

- Electronic Frontier Foundation
  - <http://www.eff.org/>
- Electronic Privacy Information Center
  - <http://epic.org/>

18