Chapter 3: Privacy

Privacy

Key Aspects of Privacy:

- Freedom from intrusion (being left alone)
- Control of information about oneself
- Freedom from surveillance (from being tracked, followed, watched)

Privacy Risks

- Intentional, institutional uses of personal information
- Unauthorized use or release by “insiders”
- Theft of information
- Inadvertent leakage of information
- Our own actions

New Technology, New Risks

- New tools for surveilance.
- Increased storage size and duration.
- More interactions that can be recorded.
- Earlier/younger access to Internet.
- Lack of public knowledge about data types and uses.
- Complicated agreements with service providers.

Fourth Amendment

The right of the people to be secure in their person, 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.

Technology & 4th Amendment

- 4th Amendment written to limit government intrusion into homes, personal possessions, and documents.
- Much information now is not stored in homes or on physical documents, but on servers/databases we don't own.
- New technology allows new kinds of surveilance not previously regulated and harder to know is being used.

Surveilance Technology

Many forms of non-invasive but very revealing surveilance.

- phone wire taps
- particle sniffers
- imaging systems
- location tracking
- Internet traffic analysis

Supreme Court Decisions

Olmstead v. United States (1928)

- Supreme Court allowed telephone wiretaps without a court order.
- Applied Fourth Amendment to apply only to physical intrusion/objects.

Supreme Court Decisions

Katz v United States (1967)

- Supreme Court reversed its position and ruled that the Fourth Amendment does apply to conversations and that wiretaps must be approved by court order/warrant.

Supreme Court Decisions

Kyllo v United States (2001)

- Supreme Court ruled that police could not use thermal-imaging devices or any device “not in general public use” to search a home from the outside without a search warrant.

Wire-tapping Laws

- Telephone
  - 1934 Communications Act prohibited interception of messages
  - 1968 Omnibus Crime Control and Safe Streets Act allowed wiretapping and electronic surveillance by police (with court order)
- Email and electronic communication
  - Electronic Communications Privacy Act of 1986 (ECPA) extended 1968 wiretapping laws to include electronic communications, restricts government access to email

Data Gathering

data mining: identifying patterns and relationships within large databases through the use of advanced statistical methods.

data broker: company whose primary focus is on gathering data about individuals and selling it to client organizations.

transactional data: information about an individual's interaction with digital content.

Uses of Data

- Targeted advertisements
- Software personalization
- Research studies
- Fraud detection
- Criminal investigation methods

Social Networking

- Services are often free to users but ad-supported or profit off of data gathering.
- Types and amounts of data gathered may change without users being aware.
- Social nature can distract users from possible uses of the data they provide.

Opt-in/Opt-out

Two common methods/policies for acquiring user consent:

- opt in: collector of the information may gather/use information only if person explicitly states permission.
- opt out: user must request that an organization not gather/use information, but default is to collect and use.

Control Over Personal Data

- Should companies be required to release copies of gathered data to the individual it is about?
  - Ireland's Data Protection Act (1988) requires this.
- Do individuals have a “right to be forgotten” from search results and data gathering?
  - European Union court decision in 2014 guaranteed right to be forgotten from search results.

Encryption

encryption: encoding messages or information in such a way that only certain people can read it.

symmetric encryption: a system in which the same “key” is used to encode and decode the message.

asymmetric encryption: a system in which one “key” is used to encode and a different matched “key” is used to decode.

Public-key Encryption

- Asymmetric encryption method where one key is kept private and is paired with a key that is made public.
- Others can use public key to encrypt and be sure only key owner can read it.
- Key owner can use private key to encrypt to prove that they wrote the message, called a **digital signature**.

Government Control of Encryption

- U.S. ban on exporting strong encryption methods in the 1990s, lifted in 2000s.
- Some countries require encryption “back doors” in software to be able to perform “wire taps” on communications.

Anonymity

anonymous: when no name is attached to a writing, speech, artistic work, or action.

pseudonymous: when a false or fictitious name is attached to a writing, speech, artistic work, or action.

Anonymity

- Many famous past writings done anonymously or pseudonymously.
  - Common Sense, Federalist Papers, Gulliver's Travels, and Jane Eyre
- Supreme Court has ruled that laws and law enforcement cannot punish people for remaining anonymous, if their actions were otherwise legal.

Arguments for Anonymity

- *"Anonymity is a shield from the tyranny of the majority"* -Supreme Court, 1995
- Protects people from unfair backlash.
- Allows people to avoid abusers.
- Can help users avoid unwanted data tracking.

Arguments Against Anonymity

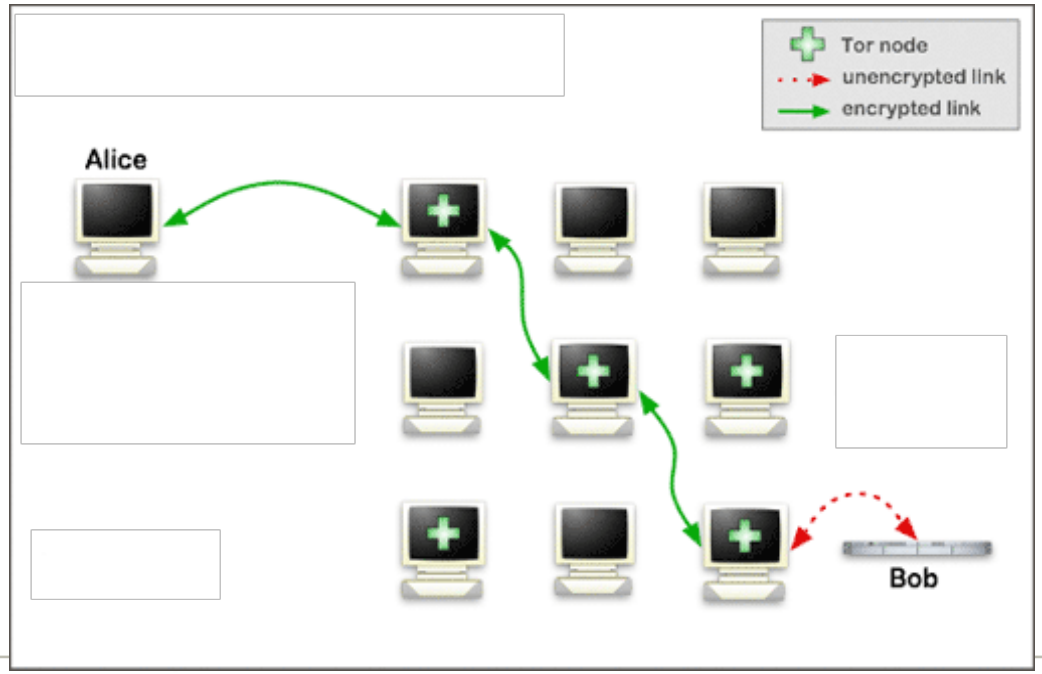
- Allows harassers/abusers to avoid repercussions.
- Can be used to conceal criminals' identities.
- Opens up more opportunities for fraud.
- Could conceal illegal surveillance by law enforcement.

Tor Networks

- Tor Network: The Onion Routing Network
- Conceals IP address by routing messages through multiple “nodes.”
- Uses layers of encryption like an onion.

Tor Algorithm

- The message passes through multiple nodes, only knowing the IP of the nodes before and after.



Tor Algorithm

- The message is encrypted with the public key of each node on the route.
- Each decrypts with its private key and gets the IP of the next node to send to.