Law, Ethics, and Privacy
Lesson Introduction

- Understand **laws that are relevant** to cyber security.
- Learn about **professional and ethical conduct** in the context of cyber security.
- Gain an understanding of **privacy challenges in the online world**.

US Laws Related to Online Abuse

- **Cyber crime**
  - Data theft, identity theft, extortion etc.
- **Copying and distribution of digital objects (software, music)**
  - Copyrights, patents, trade secrets.
  - How are these applicable in the context of digital/computer objects?
- **Privacy**
  - Who can collect my information, how can I control it, how could it be used etc.?

US Computer Fraud and Abuse Act (CFAA)

- Defines **criminal sanctions** against various types of abuse

- Unauthorized access to computer containing:
  - data protected for **national defense**
  - banking or **financial information**

- Unauthorized access, use, modification, destruction, disclosure of computer or information on **a system operated by or on behalf of US govt.**

US Computer Fraud and Abuse Act (CFAA)

- Accessing without permission a protected computer (**any computer connected to the Internet**)
- Transmitting code that causes damage to computers (**malware**)
- **Trafficking in computer passwords**

Digital Millennium Copyright Act

(Intellectual Property: Music, software piracy)

- Digital objects **can be copyrighted.**
- It is a **crime to circumvent or disable anti piracy functionality** built into an object.
- It is a **crime to manufacture, sell, and distribute devices that disable anti piracy functionality** or copy objects.

Digital Millennium Copyright Act

(Intellectual Property: Music, software piracy)

- **Research, educational exclusions** (e.g., libraries can make up to three copies for lending).

- RIAA lawsuits & P2P music sharing – electronic frontier foundation

Computer Abuse Laws Enforcement

Challenges:

- **Enforcement is difficult**
  - Attribution is hard (evidence collection, forensics etc.)
- Transnational nature of the Internet
- **Cyber criminal ecosystem evolves** to undermine legal safeguards

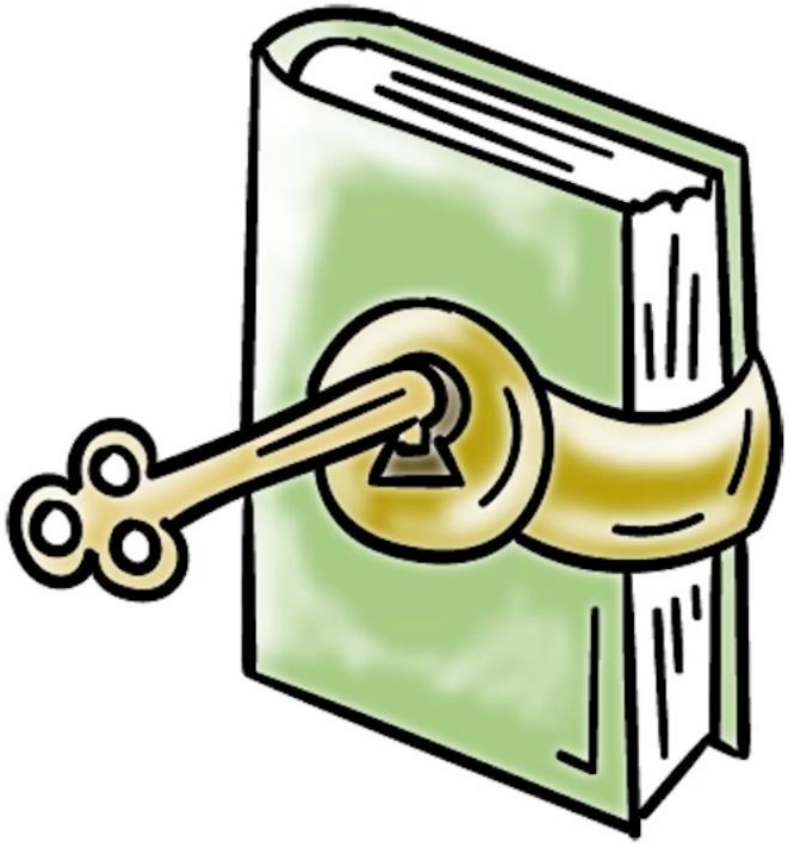
Ethical Issues

Difference between law and ethics

- **Individual standard vs. societal**
- No external arbiter and enforcement unlike law
- **Examples** – What do you do when you discover a vulnerability in a commercial product? Ethical disclosure?
- Code of ethical conduct (IEEE, ACM, university)

Ethics: expected behavior, how do we normally act in our society, how to act as a "good person".

Privacy



Definition: A user's ability to control how data pertaining to him/her can be collected, used and shared by someone else.

Privacy

- **Privacy is not a new problem.**
  - People have always worried about what others (friends, enemies, governments) might know about what they do.

- Scale and magnitude at which information about us and our activities can be **collected**, ways in which it can be **used**, and shared or sold.

Privacy

What is private?

- **Financial** statements, credit card statements, banking records etc.
- **Health/medical** conditions
- **Legal** matters
- **Biometrics** (e.g., fingerprints)
- **Political** beliefs
- **School and employer records**
- **Web browsing habits**? What do we search, what do we browse? Websites we visit?
- **Communication** (emails and calls)
- **Past history** (right to be forgotten)

Privacy

What is not private?

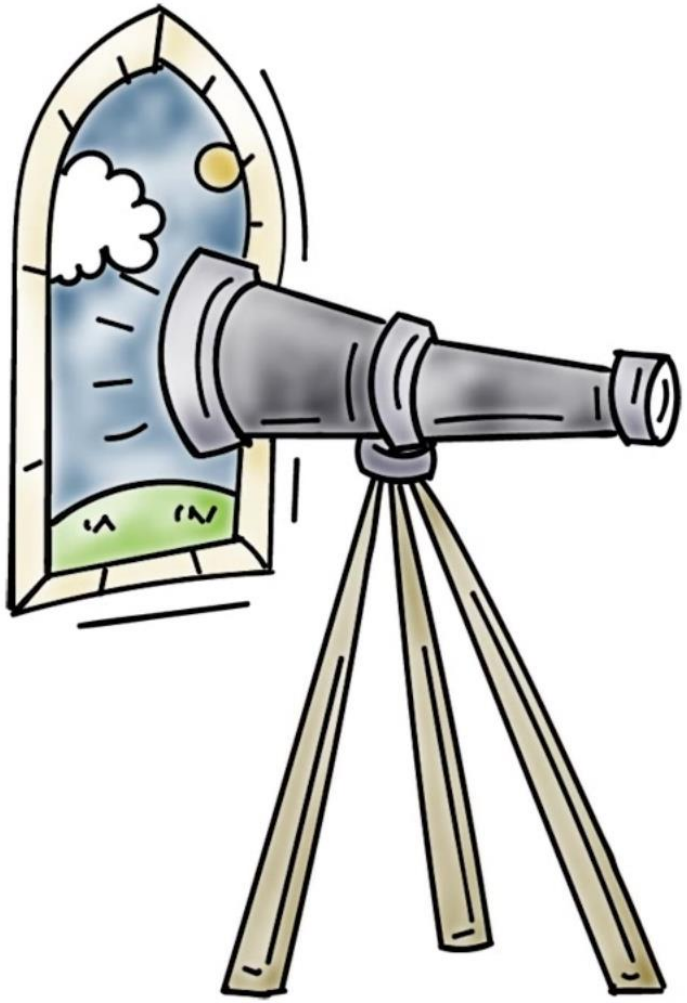
- Where I live? My **citizenship**?
- I am **registered to vote**? (US)
- My **salary** (state employee because Georgia Tech is a public university)

Privacy

- Do we need privacy only for individuals?

- **Universities, hospitals, charities** require privacy and need to protect data of people they serve or have as employees.

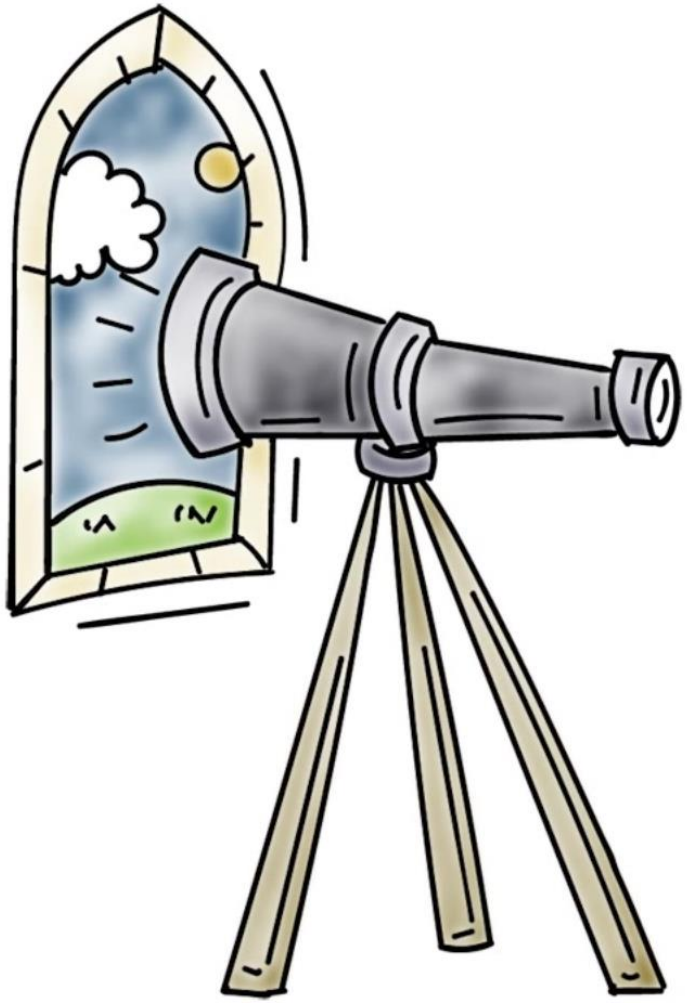
Threats to Privacy



- **Traffic analysis** (we know who you talk to)
- **Surveillance** (scale and magnitude – cameras everywhere, Snowden disclosures) we are all subject to be monitoring.
- **Linking and making inferences** (big data, data mining, analytics)

Tracking of phones or credit cards are ubiquitous. But it does not mean that people are interested in what "you" as an individual are doing. Most of the time, people are learning your behavior to serve you better or provide you customized information.

Threats to Privacy



- **Social media** (we know your friends)
- **Tracking of web browsing** (cookies)
- **Location aware applications** (we know where you have been)
- Sometimes **we are willing parties** (loyalty cards in stores)

Privacy Threats to Online Tracking Info

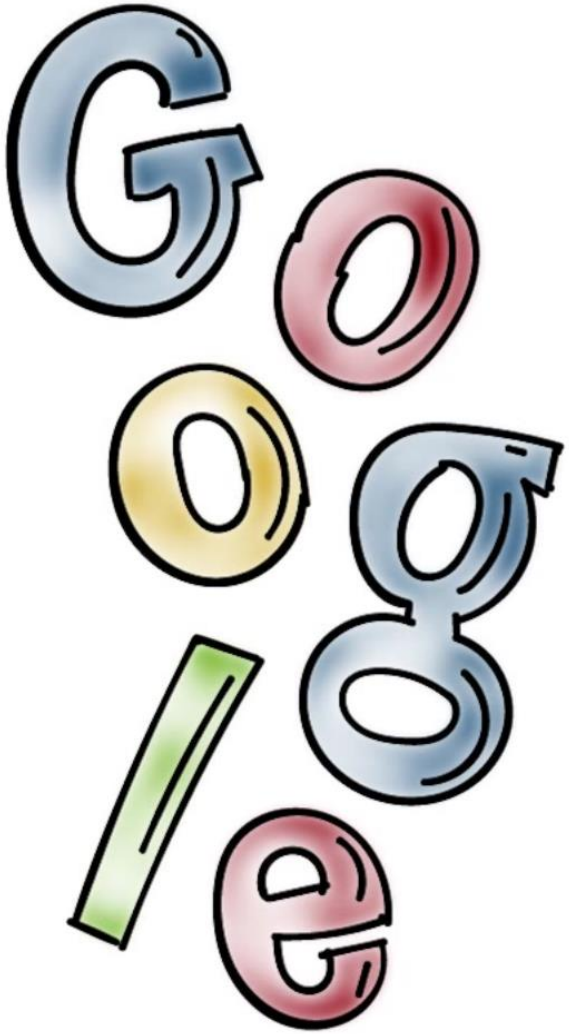
- Collection of **information about you** (e.g., tracking) – with or without your consent?
- **Usage** – only used for specified purpose you agreed to?
- **Information retention** – how long can they keep it?
- **Information disclosure and sharing** – disclosed to only authorized or agreed to parties?
- **Privacy policy changes** – can information collector/holder change to a more lax policy without your agreement?
- **Information security** – identity and access management, monitoring, secure against various threats we discussed.

Example: Google Privacy Policy

What information is collected about you?

- **Personal information** like name, email address, credit card, telephone number etc. that we provide to create an account. Profile?
- **Services** we visit a certain a website. Use it for advertising.
- **Device information**: hardware model, OS, network information (IP address) etc.
- **Search queries**
- Who we **call**? For long we talk?
- **Cookies**
- **Location** information
- **Applications**

Example: Google Privacy Policy



How is collected information used?

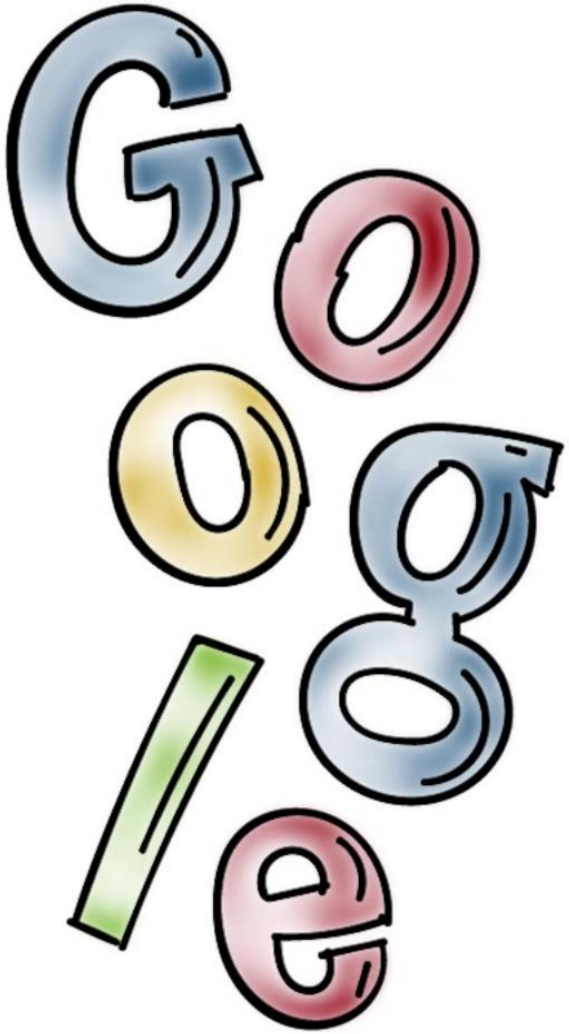
- Improve user experience (**personalization**)
- For serving you **targeted advertisements** (this is how they make their money) – we can set ad preferences.

Example: Google Privacy Policy

Who do they share it with?

- **With opt-in,** can share with companies, individuals and organizations outside of Google.
- **Domain administrators and resellers** who provide user support to your organization can get certain information about you that you give to Google.
- **Affiliates and other trusted businesses** or persons with appropriate confidentiality and security measures.
- For **legal reasons**.

Example: Google Privacy Policy



Information security

- Many services use encryption
- Stronger authentication (two factor)
- Other safeguards

Changes to privacy policy

- Will not reduce user rights without your consent

Facebook Privacy Policies

Do companies adhere and operate according to the privacy policy you gave consent to?

Not really, Facebook had issues and actually the United States Federal Trade Commission went after it for violation of user privacy.

Facebook Privacy Policies

What did it do or did not do?

- Made information users designated as private – friend list – **public without consent**
- Made personal information available to applications of friends
- **Shared information with advertisers** that it had promised not to share
- Verified apps were **not really verified**

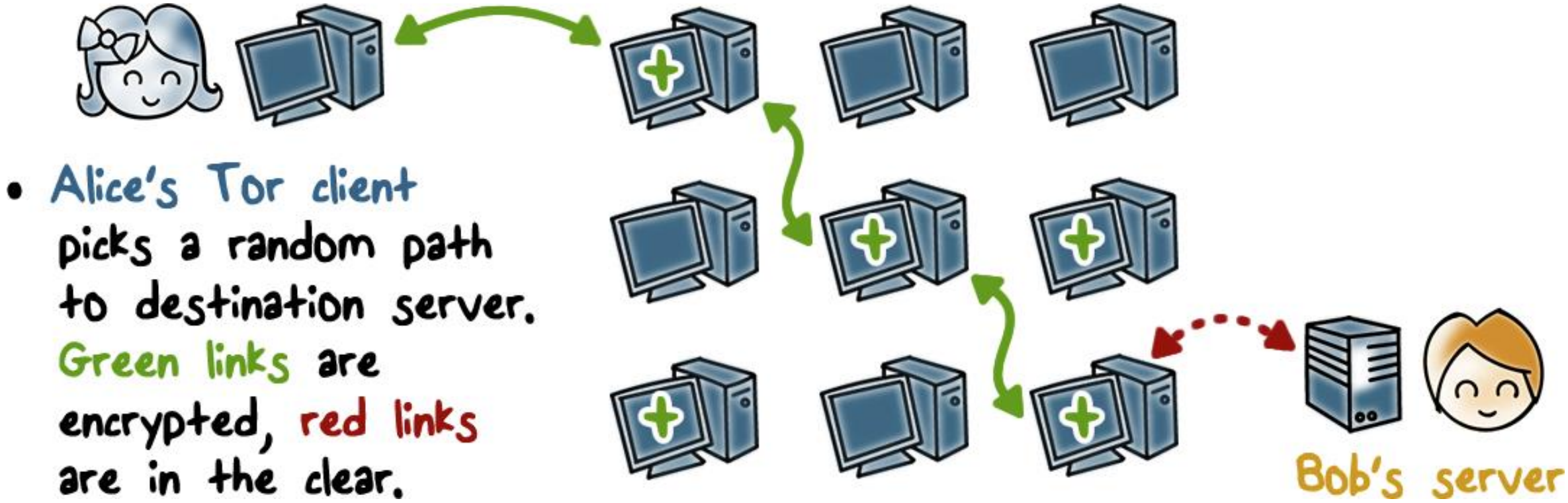
FTC Sanctions

Consequences of privacy policy violation:

- **3rd party privacy audits** every 2 years for the next 20 years
- **Prohibited from misrepresenting privacy** and security setting provided to consumers
- **Obtain affirmative express consent before sharing user information** in a way that exceeds their privacy settings

Privacy Enhancing Technologies

- **Tor** (network traffic analysis would not allow someone to know where we are coming from)
  - Alice does not want web service to know she is accessing it.



Privacy Enhancing Technologies

TOR: Onion routing is the basic idea

- With the help of a directory service, get a set of nodes
- Random set and order
- Alice prepares a message and creates onion layers with encryption

- **Pseudo-anonymity** (fake or fictional identities), multiple identities etc.
- **Aggregation, privacy enhancing transformations** (generalization, anonymizing, diverse data values etc.)

Controlling Tracking on the Internet

- Third party **cookie blocking**
- **Do not track**
- Clearing client's state
- **Blocking popups**
- Private browsing

Law, Ethics, and Privacy
Lesson Summary

- Computer fraud and abuse laws **aim to go after malicious actors** but many of their provisions have led to **plenty of debate**
- Ethical standards and professional code of conduct specifies **what online activities are out of bounds**.
- Online privacy is a **huge issue** for many but **we do not seem to have much of it**.