A GIFT OF FIRE THIRD EDITION - SARA BAASE
CHAPTER 3: Technology & Free Speech

Lecture 2

Syada Tasmia Alvi

Lecturer, Dept.of CSE

Daffodil International University

Anonymity

❏ True anonymity

  ○ "Unlinkability"

  ○ Inability of anyone to determine the true author's identity

  ○ Legally problematic

Anonymity

❏ Pseudonymity:

   ○ Pseudonymity is the near-anonymous state in which a user has a consistent identifier that is not their real name: a pseudonym.

   ○ public pseudonyms: link between pseudonym and human being is easy for the public to know or discover

   ○ non-public pseudonyms: link known by sysadmins, but no one else

   ○ unlinkable pseudonyms: link not known and not discoverable by service operators

Anonymous Re-mailers and Web Browsers

❏ Johan Helsingius set up the first well-known anonymous email service in Finland in 1993.

   ○ Users were not entirely anonymous

   ○ the system retained identifying information.

   ○ Return address stripped off and then forwarded to recipient

❏ To send anonymous email using a "re-mailer" service, one sends the message to the remailer, where the return address is stripped off and the message is re-sent to the intended recipient.

❏ Anonymous web browsers - hide user's IP address, do not track or store activity

Anonymity vs. Community?

❏ Supporters of anonymity

  ○ Claim that it is necessary to protect privacy and free speech.

  ○ Helps those who are concerned about political or economic retribution.

    ■ Human rights workers

    ■ Victims of domestic violence

Anonymity vs. Community?

❏ Opponents of anonymity

    ○ Claim that it is anti-social and allows criminals to hide from law enforcement.

    ○ Threatens civil discourse ("marketplace of ideas")

    ○ Examples:

        ■ Online harassment

        ■ Fraud

Spam

- ❏ Unsolicited, mass e-mail

  - ○ Is cheap to senders but may impose costs on recipient's time or the recipient's online account (or both).

  - ○ May contain objectionable content (political, commercial ads, solicitations for funds, pornography, etc.)

  - ○ May contain a disguised return address.

  - ○ May pass through filters.

- ❏ – Invades privacy.

- ❏ – Creates a financial and managerial burden on ISPs.

Spam: solutions (?!)

- ❏ Technology: Filters that screen out spam.

- ❏ Market pressure: Services that list spammers

- ❏ Small "microfee" for sending an email?

- ❏ requires consent for email marketing

- ❏ Vigilantism: Punish spammers

Thank You