CS 4930/5930: Arguments/Definitions

Yanyan Zhuang
Department of Computer Science
http://www.cs.uccs.edu/~yzhuang/

Part I: Privacy and Anonymity

- We are NOT anonymous by default
  - My IP address can be linked directly to me
    - ISPs store communication records
    - Law enforcement can subpoena these records (phone records, location data, IP, email, text messages, cloud data, social media, etc.)
  - My browser is being tracked
    - Cookies, HTML5 storage, etc.
    - Browser fingerprinting
  - My activities can be used to identify me
    - Unique websites I visit, and apps I use
    - The links I click

https://www.propublica.org/article/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data

Why use anonymous systems?

- “If you are not doing anything wrong, you shouldn't have anything to hide”
  - Only if you are doing something wrong should you worry, and then you don’t deserve to keep it private
  - http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html

Why use anonymous systems?

- “If you are not doing anything wrong, you shouldn't have anything to hide” -- counter arguments:
  - “So do you have curtains?” “Can I see your credit-card bills?”
  - “I don’t need to justify my position. You need to justify yours. Come back with a warrant.”
  - Show me yours and I’ll show you mine.

Why use anonymous systems?

- “If you are not doing anything wrong, you shouldn't have anything to hide”
  - Nothing-to-hide argument’s extreme form: assume anonymous communications are for criminals (hiding bad things), but
    - Medical conditions
    - Associations with other individuals
    - Political opinions

Why use anonymous systems?

- “If you are not doing anything wrong, you shouldn't have anything to hide”
  - Less extreme form: privacy interest is minimal, and the security interest in preventing terrorism is much more important
    - Privacy might be invaded if you’re watched, even if no secrets are revealed
    - Creepy regardless of whether the peeper finds out anything sensitive or discloses any information to others
      - “1984”, George Orwell

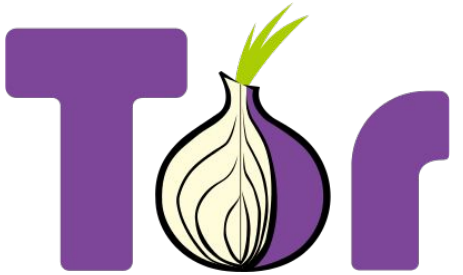
Why use anonymous systems?

- “If you are not doing anything wrong, you shouldn't have anything to hide”
  - “Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say”. --- Edward Snowden

Who uses anonymous systems?

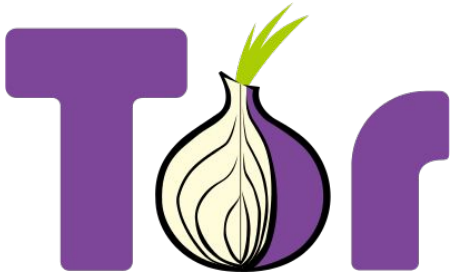
- Fact: who uses Tor?
  - Journalists
  - Human rights activists
  - Abuse victims
  - Business executives
  - Law enforcement
  - **Normal people**

What is Tor?



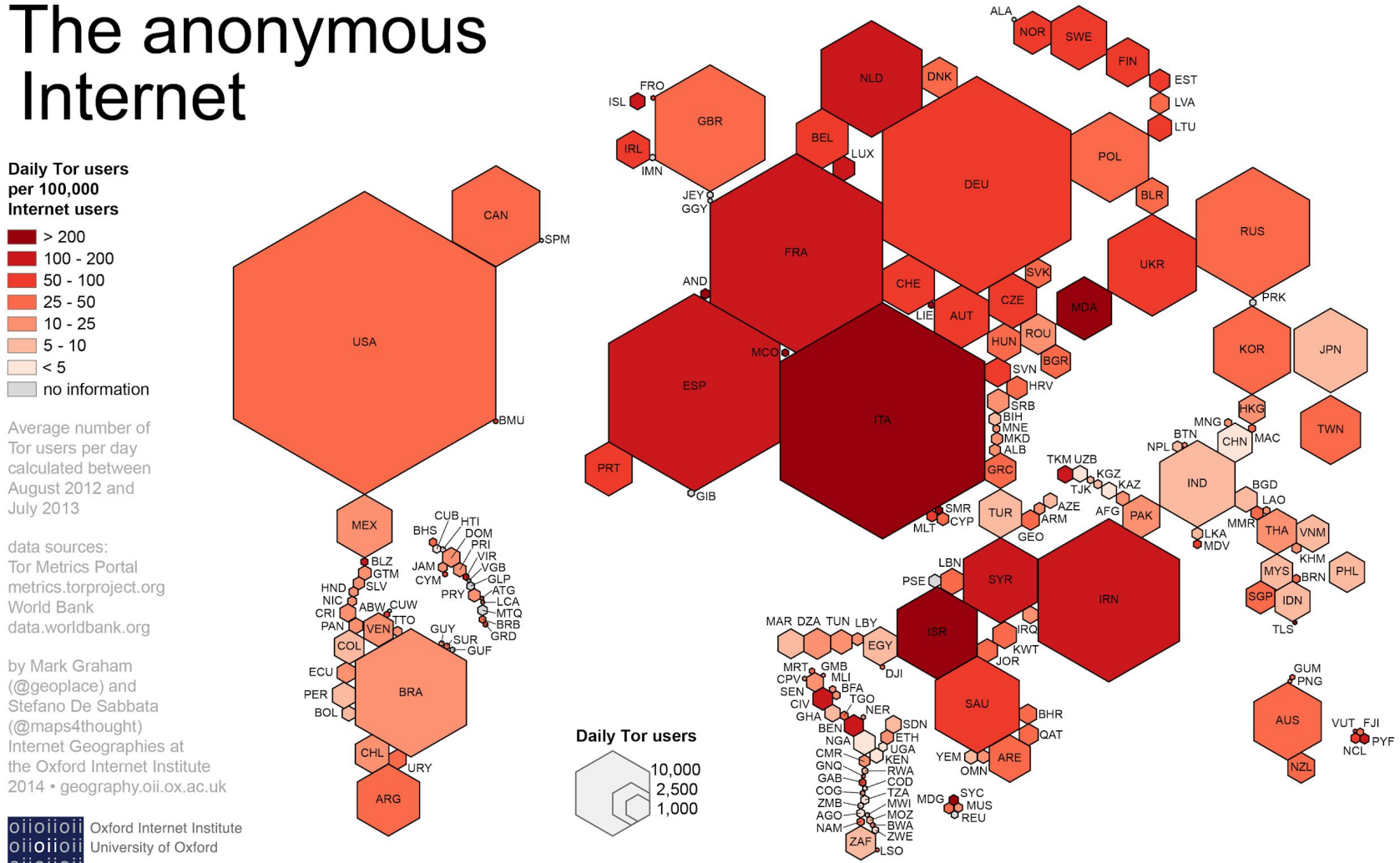
- Tor (The Onion Router) is free software for enabling anonymous communication
  - Directs Internet traffic through a worldwide overlay network to conceal a user's location
    - Makes it difficult to trace Internet activity
    - Does not prevent inference when a service being accessed through Tor

What is Tor?



- Tor (The Onion Router) is free software for enabling anonymous communication
  - Encryption in the application layer, nested like the layers of an onion
    - Encrypts data, including the next node IP address, sends it through a virtual circuit comprising successive, random Tor relays
    - Each relay decrypts a layer of encryption to reveal the next relay's IP in the circuit to pass the remaining encrypted data
    - The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address

The anonymous Internet



Why do we want privacy and anonymity?

- To protect privacy
  - Avoid being tracked by advertising companies
  - Viewing sensitive content
    - Information about medical conditions
    - Content that certain governments deem sensitive
- Avoid prosecution
  - Not every country has freedom of speech
  - Or... doing something illegal (don't do it!)
- Prevent chilling-effects
  - Self-censorship

Definitions: Privacy and Anonymity

- Privacy (1)
  - "The right to be left alone," in a person's sphere of existence they should be free of coercion, constraint, and uninvited observation. (Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, 4 (5), (1890))

Definitions: Privacy and Anonymity

- Privacy (1)
  - "The right to be left alone," in a person's sphere of existence they should be free of coercion, constraint, and uninvited observation. (Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, 4 (5), (1890))
  - Drawback: defining the "sphere of existence" and its limits

Definitions: Privacy and Anonymity

- Privacy (2)
  - Privacy as "secrecy," a definition in which information is either private (secret) or public.
  - Secrecy is about keeping the information away from others

Definitions: Privacy and Anonymity

- Privacy (2)
  - Privacy as "secrecy," a definition in which information is either private (secret) or public.
  - Secrecy is about keeping the information away from others
  - Drawback: black and white protection doesn't cover nuanced situations.
    - Medical data, for example, isn't secret (it is shared with health providers), but it should still be private.

Definitions: Privacy and Anonymity

- Privacy (3)
  - Privacy as contextual integrity, a definition that uses context and societal norms about data and communications to decide if privacy has been violated
    - 5 independent parameters: data subject, sender, recipient, information type, and transmission principle.

Definitions: Privacy and Anonymity

- Privacy (3)
  - Privacy as contextual integrity
    - 5 independent parameters
      - Data subject: patient, shopper, investor
      - Sender/Recipient: bank, hospital, police
      - Information type
        - Contents of an email, data subject's demographic information, medical/financial information
      - Transmission principle
        - Consent, stolen, buying, selling, acting under the authority of a court with a warrant

Definitions: Privacy and Anonymity

- Privacy (3)
  - Assessing the privacy impact of information flows requires the values of **all five parameters** to be specified
  - Conceptions of privacy are based on ethical concerns that evolve over time

Definitions: Privacy and Anonymity

- Privacy (3)
  - Assessing the privacy impact of information flows requires the values of **all five parameters** to be specified
  - Conceptions of privacy are based on ethical concerns that evolve over time
  - Drawbacks: Societal norms change, and not always for the better. There is no real room for any level of autonomy in this definition

Definitions: Privacy and Anonymity

- Anonymity (1)
  - Anonymity
    - Unlinkability, unobservability
  - Anonymity set
    - Message could have been sent by any of K people

Unlinkability and Unobservability

- Unlinkability
  - From the adversaries perspective, the inability to link two or more items of interest
    - E.g. packets, events, people, actions, etc.
  - Three parts
    - Sender anonymity (who sent this?)
    - Receiver anonymity (who is the destination?)
    - Relationship anonymity (are sender A and receiver B linked?)
- Unobservability
  - From the adversaries perspective, items of interest are indistinguishable from all other items

Definitions: Privacy and Anonymity

- Anonymity (2)
  - Anonymity
    - Unlinkability, unobservability
  - Anonymity set
    - Message could have been sent by any of K people

How to quantify?

- Larger anonymity set → stronger anonymity

Definitions: Privacy and Anonymity

- Conclusion
  - Anonymity cares about obscuring the metadata but not the message
    - Who sent this message?
    - Who is communicating with who?
  - Privacy cares about obscuring the message but not the metadata
    - What data has been accessed?