COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

Foundations of Privacy Technology II

Information Privacy with Applications

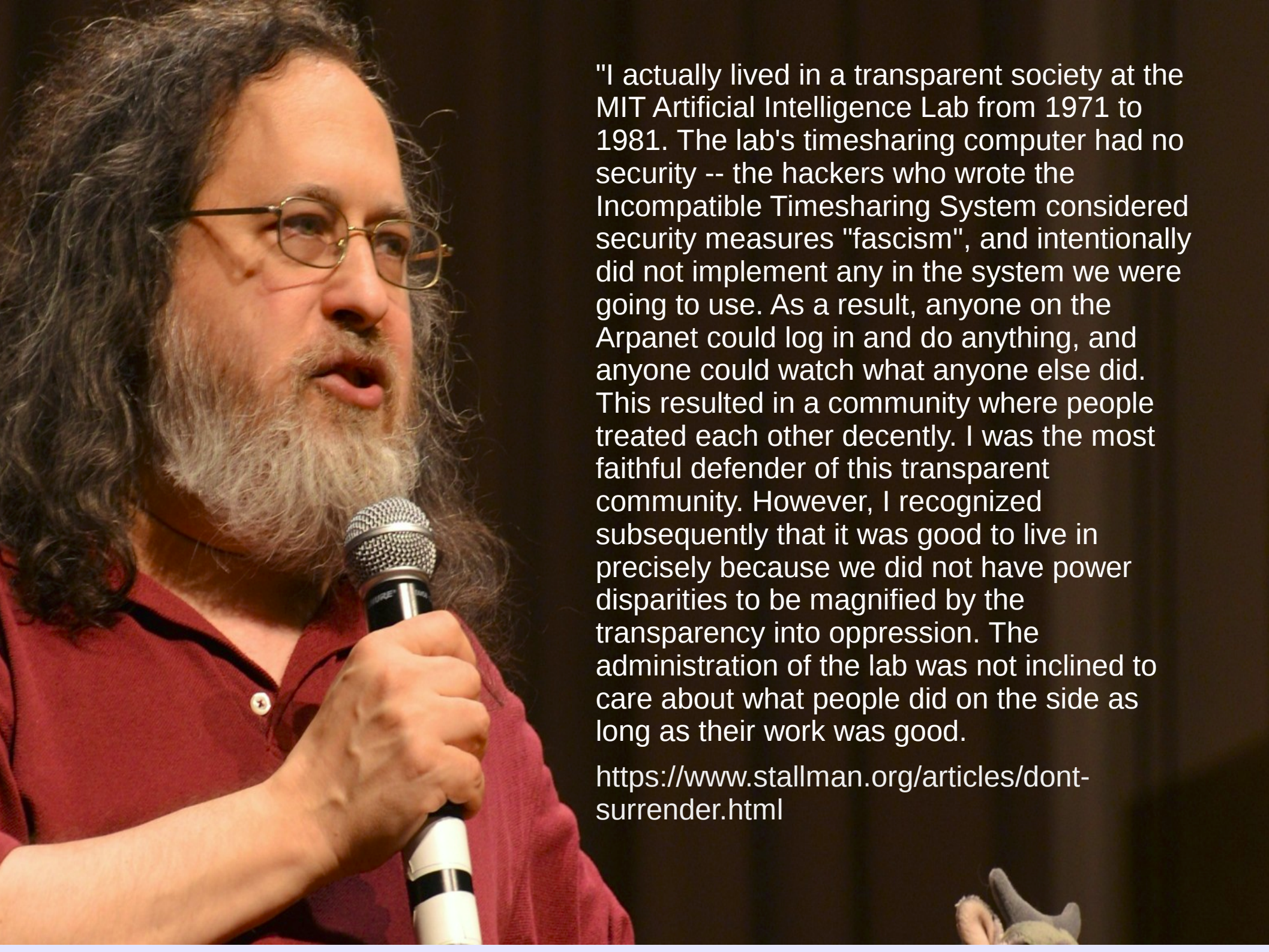
David Sidi (dsidi@email.arizona.edu)

Small mention of interesting things

- dudle

trust and privacy

“we focus on one key aspect of these technologies, namely, the kind of trust they can provide” (396)



"I actually lived in a transparent society at the MIT Artificial Intelligence Lab from 1971 to 1981. The lab's timesharing computer had no security -- the hackers who wrote the Incompatible Timesharing System considered security measures "fascism", and intentionally did not implement any in the system we were going to use. As a result, anyone on the Arpanet could log in and do anything, and anyone could watch what anyone else did. This resulted in a community where people treated each other decently. I was the most faithful defender of this transparent community. However, I recognized subsequently that it was good to live in precisely because we did not have power disparities to be magnified by the transparency into oppression. The administration of the lab was not inclined to care about what people did on the side as long as their work was good.

https://www.stallman.org/articles/dont-surrender.html

“we focus on one key aspect of these technologies, namely, the kind of trust they can provide” (396)

- “Trust” here is ersatz, making up for a deficit in social trust
- technologies “providing trust” means: making trust moot
- is there any way to help to build social trust with privacy technology?

“we focus on one key aspect of these technologies, namely, the kind of trust they can provide” (396)

- “Trust” here is ersatz, making up for a deficit in social trust
- technologies “providing trust” means: making trust moot

Not all privacy technologies reduce the perimeter of trust

- privacy vs security
- how can social trust be built with technology? (2 min)

A division among safeguards offered by privacy technologies

- Minimization of disclosure of personal data
- Enforcement of rights when personal data is disclosed

Minimization is hard, since data is useful

- Data is not just good for the individual; it’s good for society---you can’t just restrict its use without cost
  - open data in science, government
  - “Tragedy of the Data Commons”
- remember Saint RMS

Enforcing rights requires people as well as technology, so it’s hard too

- Data is already disclosed, out of technology’s hands and into people’s
  - “Information does not just want to be free, it longs to be free. ... Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor..” Eric Hughes

There are two kinds of safeguard offered by privacy technologies

- Minimizing disclosure of personal data
- Enforcing rights when personal data is disclosed

There are two kinds of safeguard offered by privacy technologies

- Minimizing disclosure of personal data
- Enforcing rights when personal data is disclosed
- What distinction that we've seen before among kinds of privacy technology is very close to the above?

From Diaz and Gürses last time

- Privacy as control: a matter of policy, which **controls data use**. Does not try to minimize trust in a third party for linkable data
  - example: privacy settings
- Privacy as confidentiality: a matter of applied mathematics, which **minimizes disclosure**. Tries to minimize trust in a third party with linkable data
  - example: PIR

From last time: Two families of privacy technologies

Soft Privacy Technologies

- Focus on compliance.
- Focus on "internal controls".
- **Assumption: a third party is entrusted with the user data.**
- Threat model: third party is trusted to process user data according to user wishes.
- Examples technologies:
  - Access control, tunnel encryption (SSL/TLS)
- "Keeping honest services safe from insiders / employees".

Hard Privacy Technologies

- Stronger focus on data minimization.
- **Assumption: there exists no single third party that may be trusted with user data.**
- Threat model: a service is in the hands of the adversary; may be coerced; may be hacked.
- Common assumption: k-out-of-n honest third parties.
- May relay on service integrity if auditing is possible.
- **Challenge: achieve functionality without revealing data!**

Slide credit: George Danezis

Another division among privacy technologies is by who is trusted

- data subjects
  - the person to whom the personal data relate
- data controllers
  - collectors and processors of data from the data subject
    - providers of a service
    - third parties
- technology developers
- “peers”
  - people you may know, or not know, who are fellow users of a privacy technology

Examples

- data subjects
  - the person to whom the personal data relate
- data controllers
  - collectors and processors of data from the data subject
    - providers of a service
    - third parties
- technology developers
- “peers”
  - people you may know, or not know, who are fellow users of a privacy technology

- SSL/TLS
- PrivacyBird
- Startpage Proxy
- PGP
- Spinner Randomized Response Technique

Minimization technologies

Communication services

- email
- online social networks
- blogs
- web pages
- instant messaging
- (storage services)
- ...

Two properties of minimization technology for communication services

- confidentiality
- three related properties: unobservability, unlinkability, anonymity

Achieving unobservability, unlinkability, anonymity involves adding an intermediary

The Fundamental Theorem of Software Engineering

"We can solve any problem by introducing an extra level of indirection."

Wheeler

Trusted relays and semitrusted relays

- Following convention, call the intermediaries ‘relays’
- there are approaches with trusted and semitrusted relays
- we’ll do this in more detail in the anonymity lectures; this will be a superficial introduction

Trusted relays

- Example: Type-0 Remailers.
  - a server keeps a dictionary between real and pseudonymous emails
  - request comes to the remailer, which forwards it, gets the response, and returns it to the user
- Example: VPNs

Semi-trusted relays

- Example: Mix-nets (Chaum, 1970s). Routing protocol with a chain of servers called ‘mixes’ that shuffle (blocks from) messages received from multiple senders, and pass them to the next node, which could be another mix. Mixes only know their neighbors.

- sidenote: inexplicably, David Chaum is not cited in the reading. He is the originator of not just mix-nets but many of the ideas we are discussing.

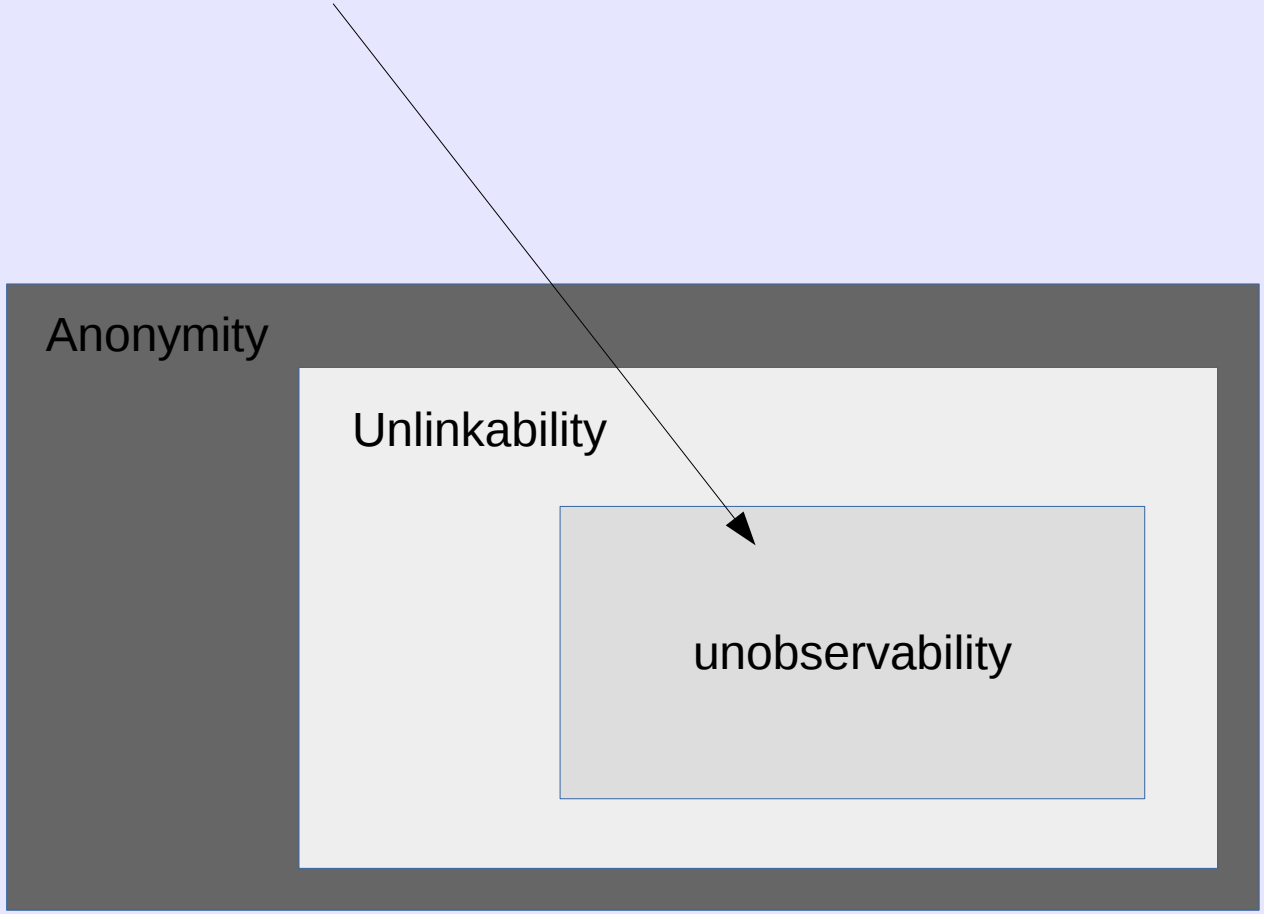
Two properties of minimization technology for communication services

- confidentiality
- three related properties: unobservability, unlinkability, anonymity
  - getting them involves an intermediary

Two properties of minimization technology for communication services

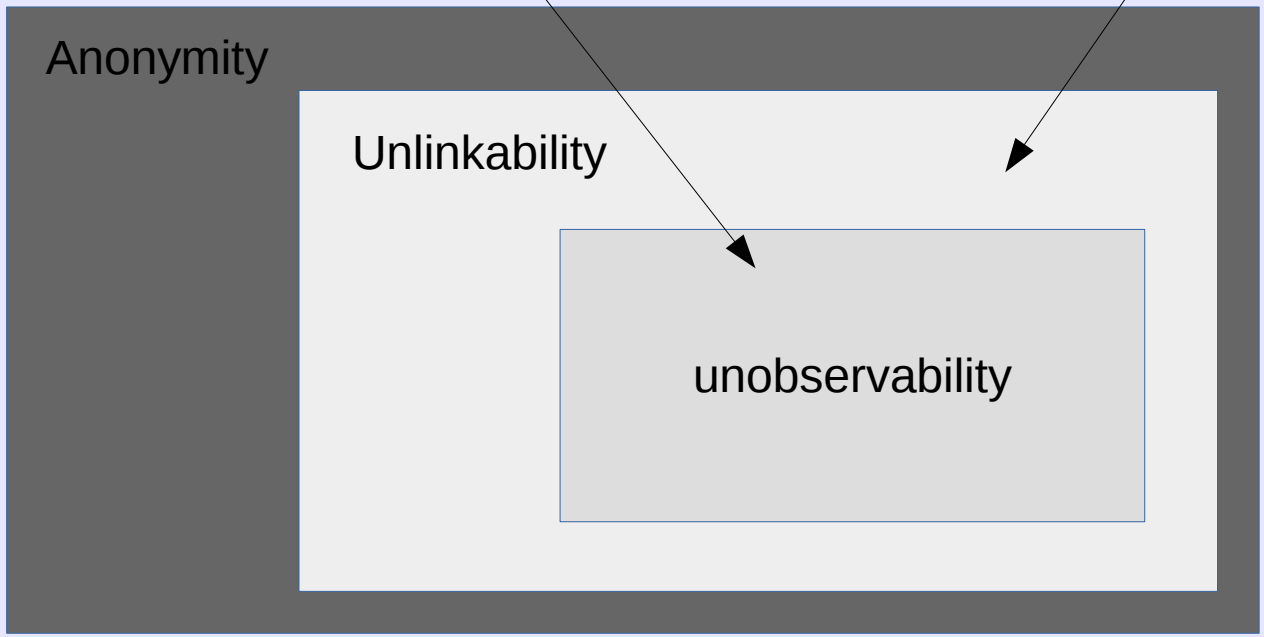
- confidentiality
- three related properties: unobservability, unlinkability, anonymity
  - getting them involves an intermediary
  - orderable by strength

can’t even tell that a message is being sent



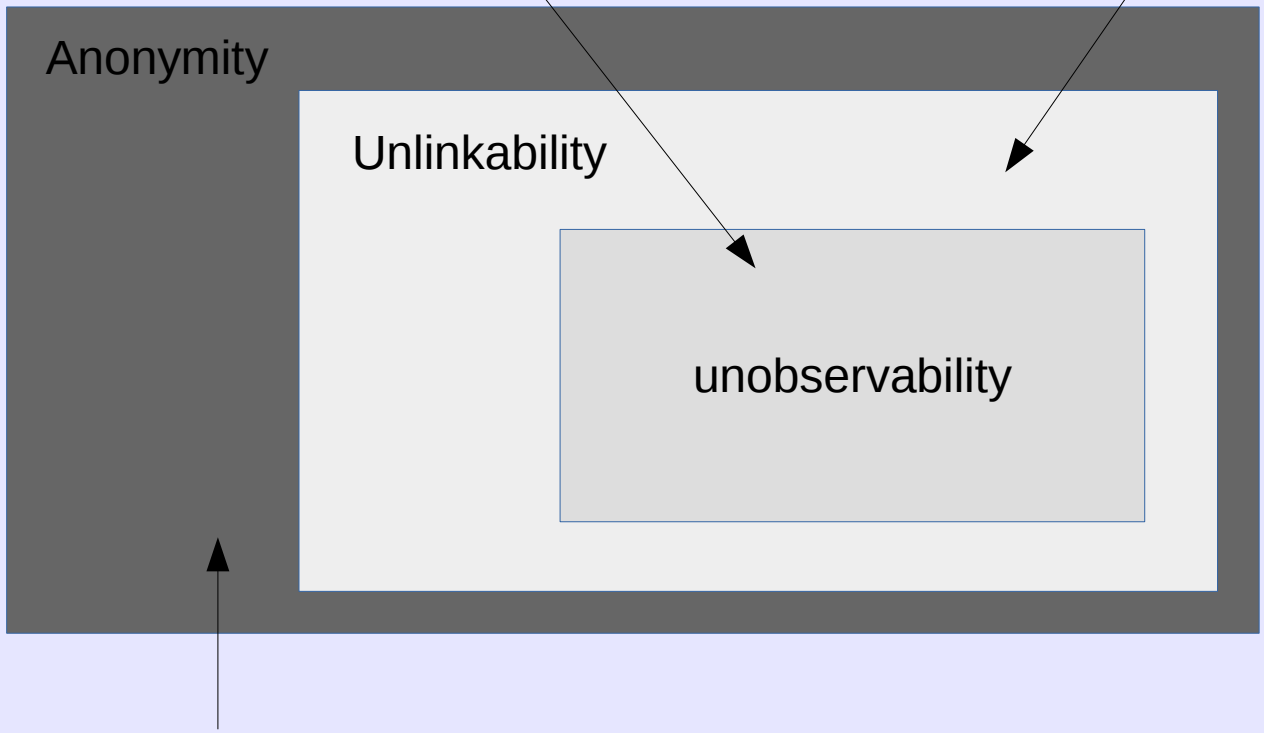
can’t even tell that a message is being sent

can tell that messages are sent, but can’t tell if messages are from the same source or different, going to the same place or different



can’t even tell that a message is being sent

can tell that messages are sent, but can’t tell if messages are from the same source or different, going to the same place or different



Can group messages by sender (receiver) but can’t identify the sender (receiver)

What is it to identify a sender or receiver? (2 min)

Anonymity set

- Anonymity is relative to a subset, called the anonymity set.
  - Think of it as answering “who might you be?”
- Can also consider the complement, “who is definitely not you?”

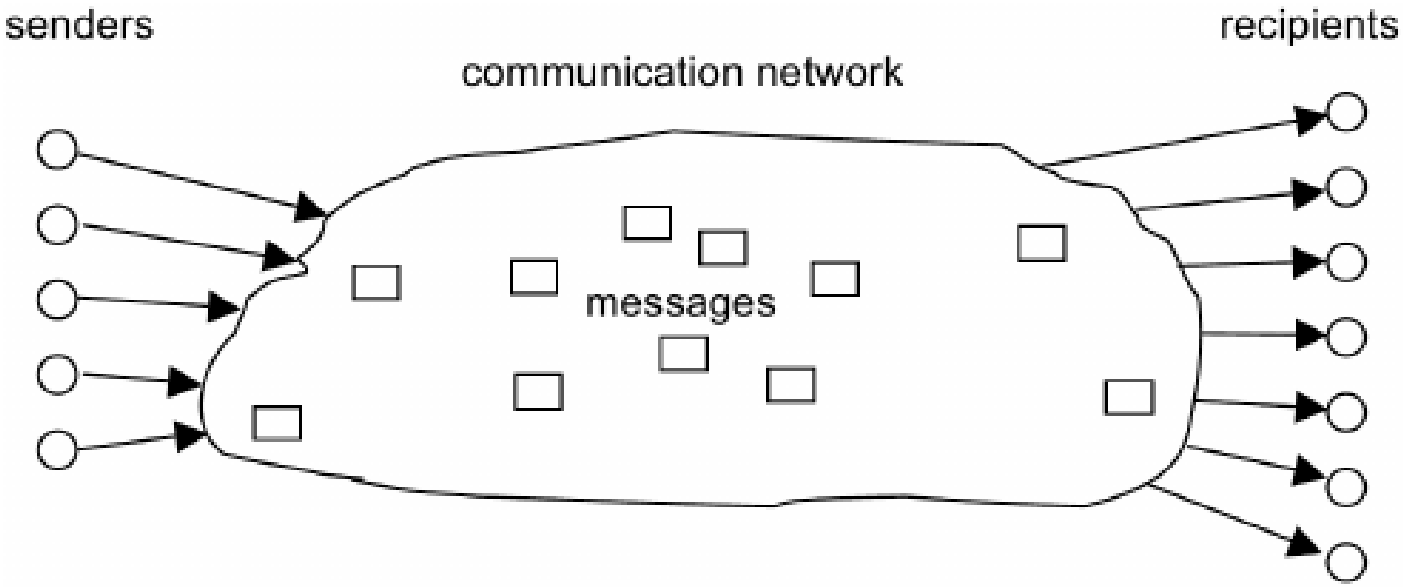
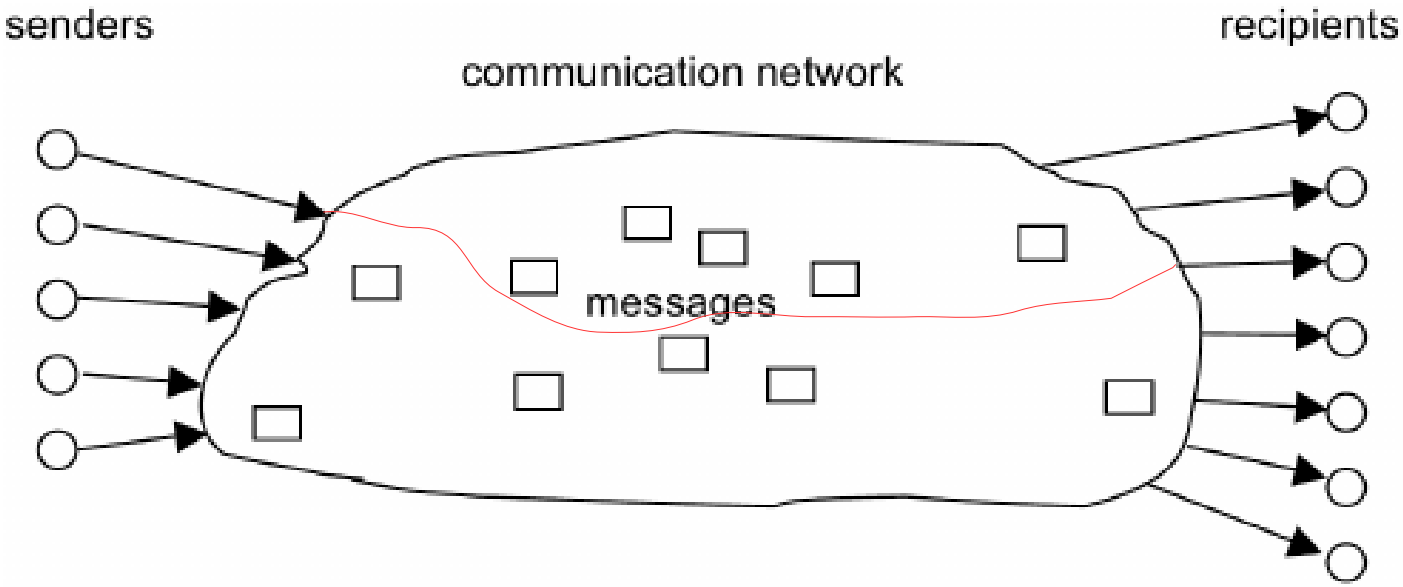
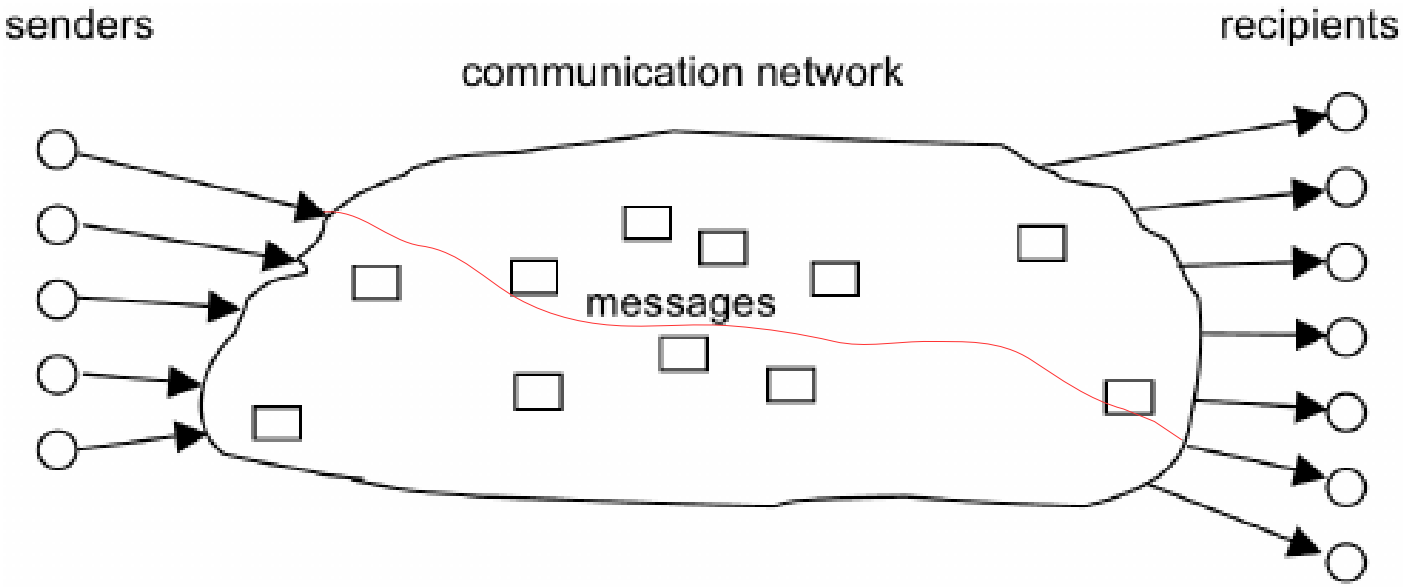
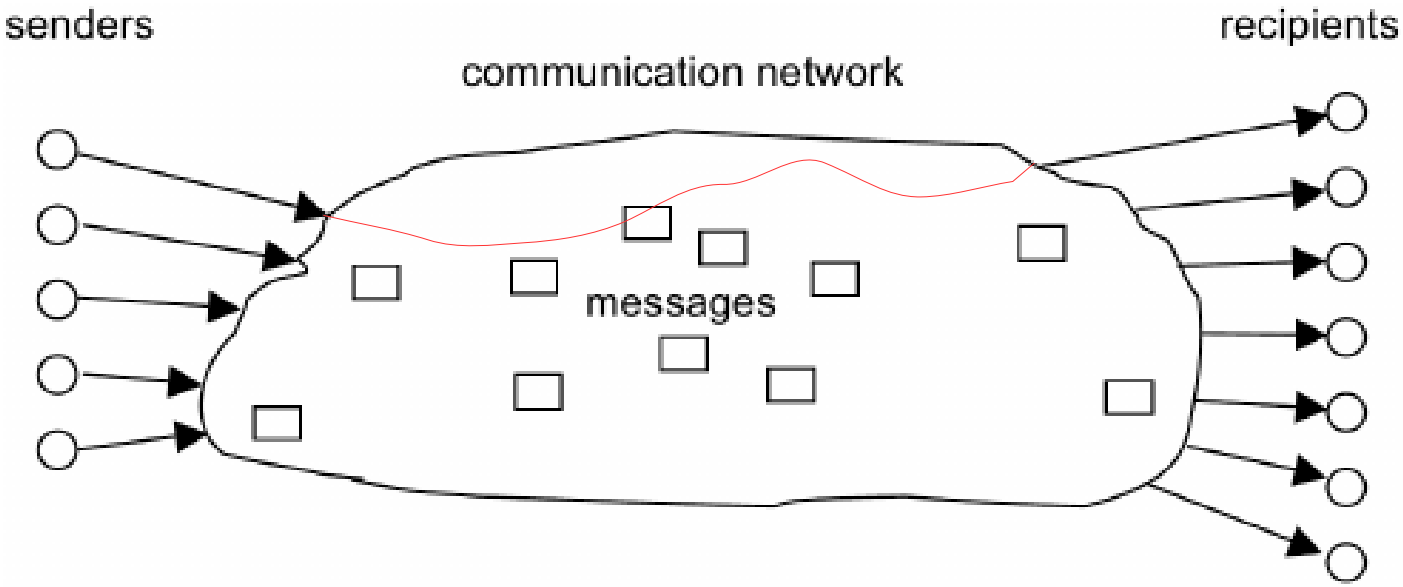
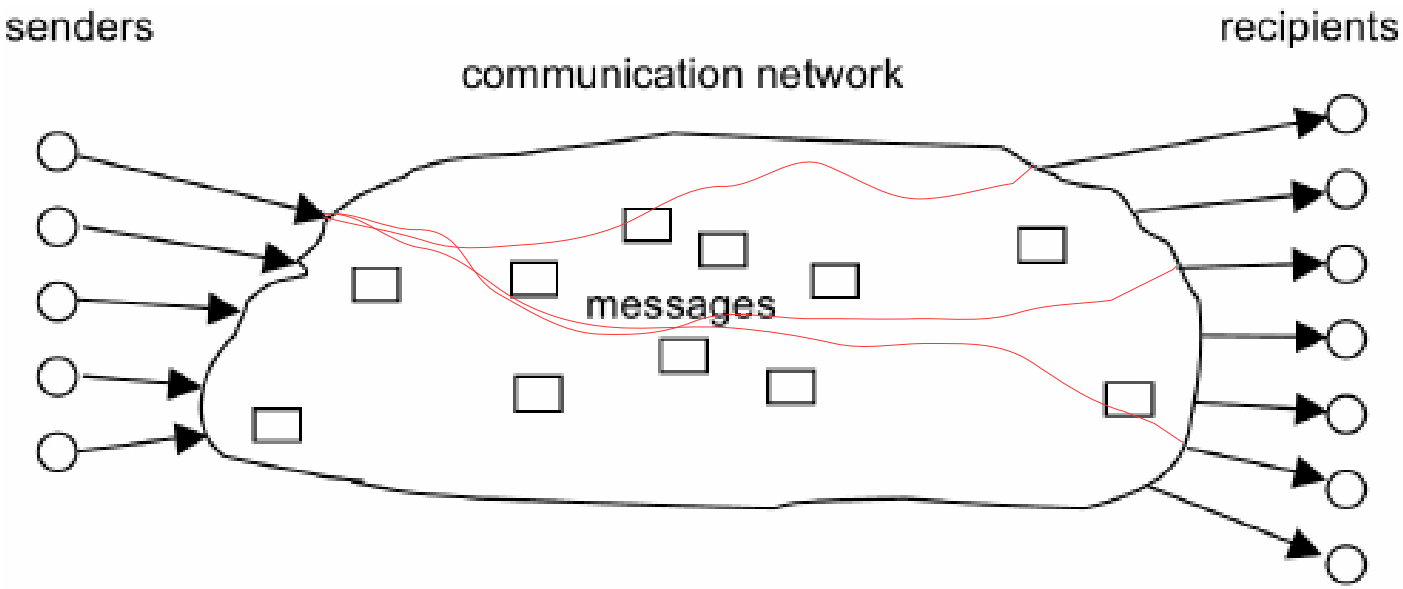


Image credit (before modification):
Christina Pöpper
Ruhr-University Bochum


senders
recipients
communication network
messages


senders
communication network
recipients
messages


senders
recipients
communication network
messages


senders
communication network
recipients
messages

Anonymity set

- Can you clearly describe the limiting cases for the anonymity set?

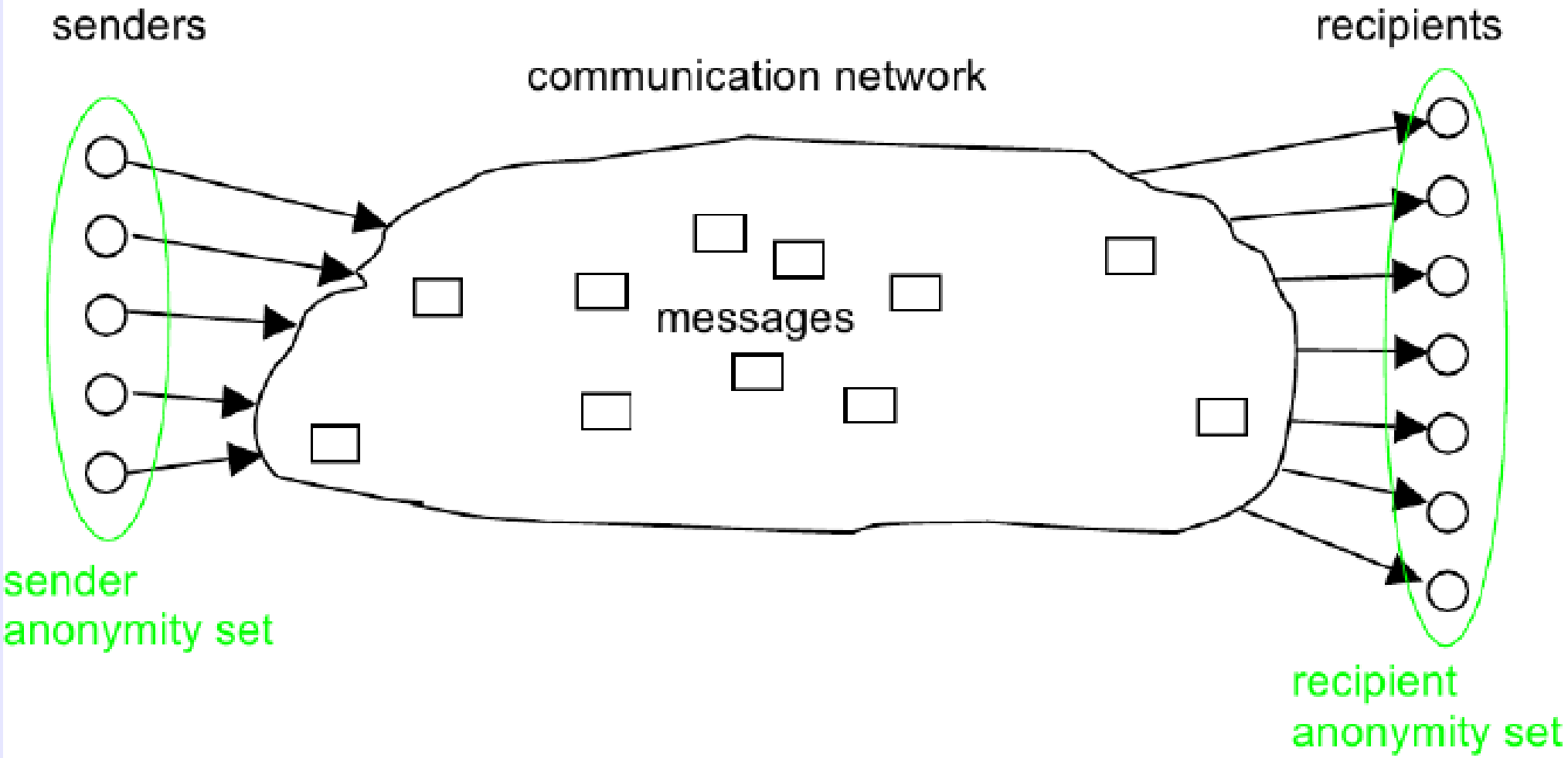


Image credit Christina Pöpper
Ruhr-University Bochum