COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

Group Privacy Technology I

Information Privacy with Applications

David Sidi (dsidi@email.arizona.edu)

Administration

- Assignment I, part II due next time
- Let’s review part I on the server
  - find
  - extra credit question: plumbing find with fd’s 1,2, and 3
  - absolute paths, and why they matter
  - permissions
  - what is in the SECRET file?

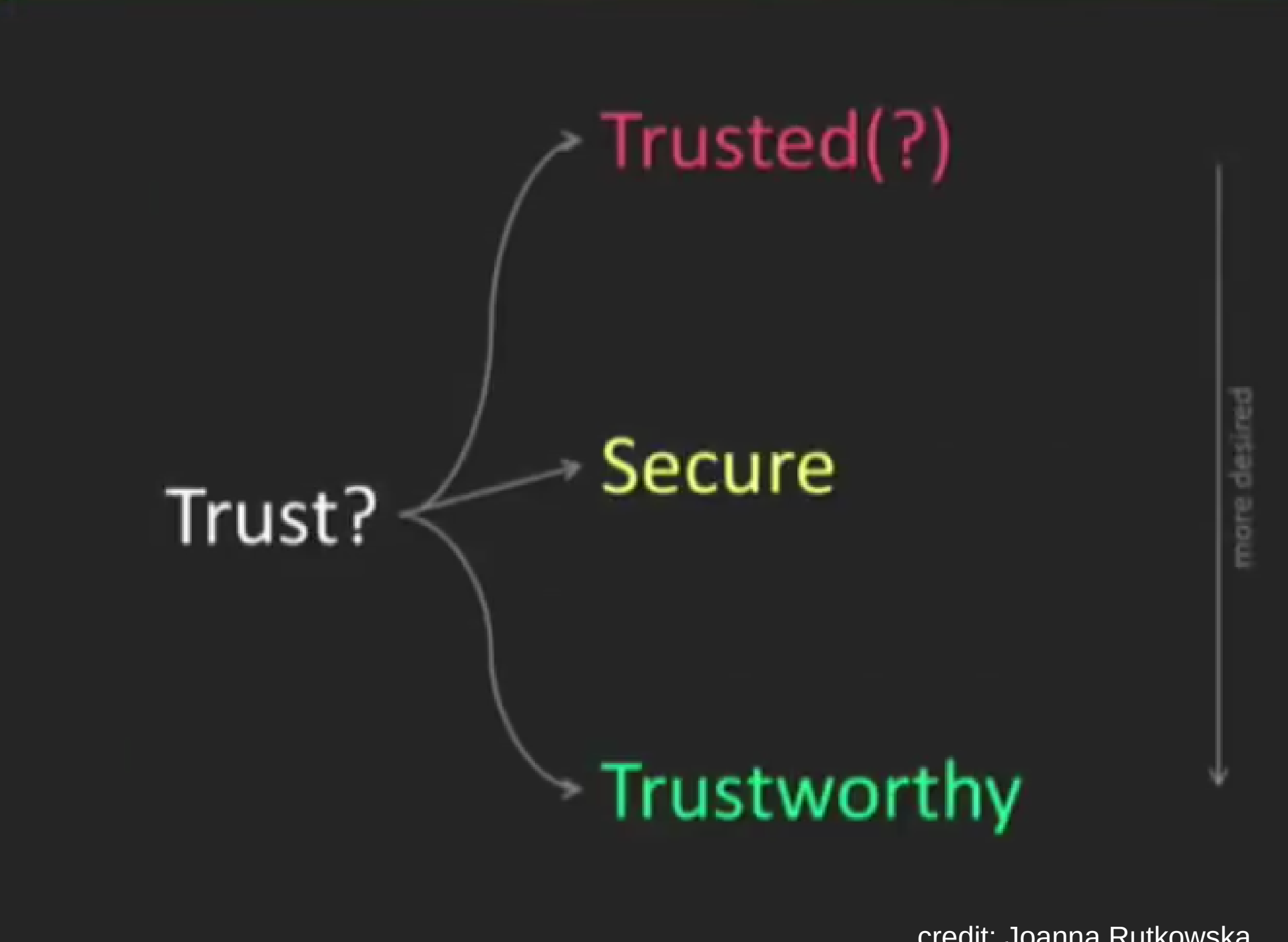
Privacy technologies as reducing the perimeter of trust

"one may argue that, at the end of the day, the main benefit of the use of privacy-enhancing technologies is to reduce the perimeter of trust." 396

- **Question: What kind of trust does he mean?**

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

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



credit: Joanna Rutkowska

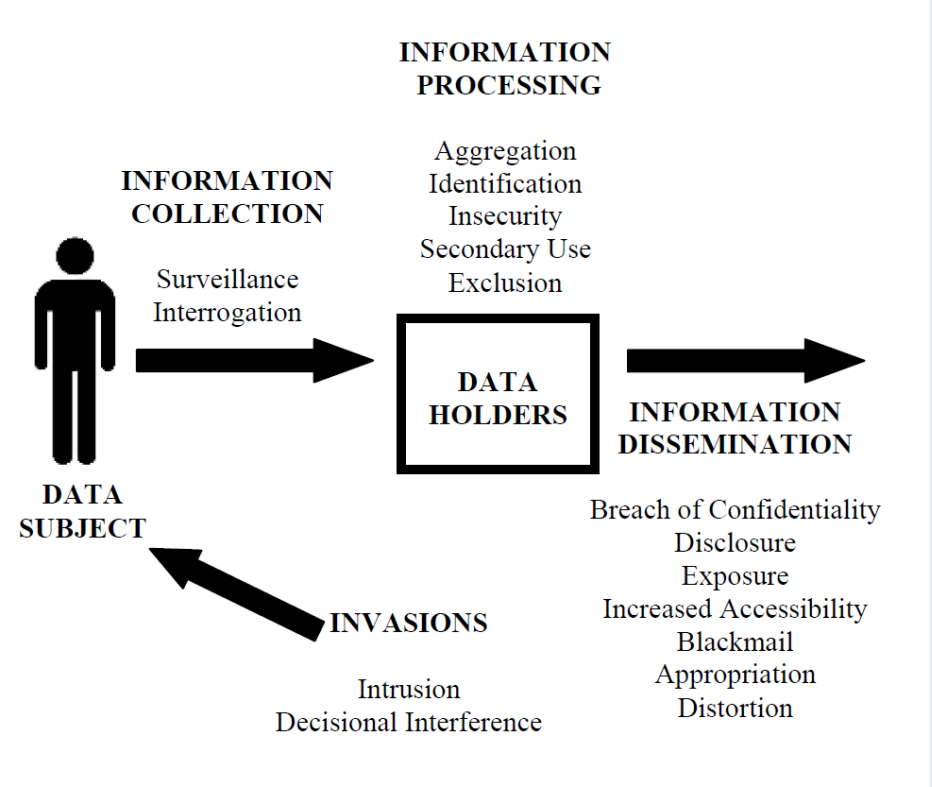

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Definitions of trust

- an assumption in a model of a system which, if false, breaks the security policy for the system (NSA definition)
- a system “whose integrity cannot be assured by external observation of its behaviour whilst in operation” (Ross Anderson, attributed as “a UK military view”)

Privacy and Harm

- One view: Information privacy is best understood by thinking about characteristic privacy harms
- Privacy technologists who subscribe to this view aim to design and implement technologies to reduce these harms, or the threat of them (we'll see how to model threats next time)
- This brings privacy research closer to security research
- See: Danezis, Solove, many more



Example harms to privacy

- A newspaper reports the name of a rape victim.
- An abusive spouse installs an app to surveil his wife
- A state government intercepts communications between a journalist and a source
- Cameras arranged in a city downtown are able to identify and track the movements of everyone who passes, and store the information indefinitely
- Reporters gain entry to a person’s home and secretly photograph and record the person without that person’s knowledge.

- A company markets a list of five million elderly incontinent women
- A company links publicly available records with aggregated private records to reveal sensitive medical information
- A company suffers a breach and leaks millions of social security numbers linked to names, addresses and more information
- Despite promising not to sell its members' personal information to others, a company does so anyway
- A government collects all internet traffic originating or passing through its country, promising not to analyze it unless there is a need at a later date

Example PETs from the reading

- Confidential communications systems: PGP, OTR, Briar, TLS
- Access systems: Idemix
- Anonymous communications systems: Tor, I2P, proxies, remailers

Privacy and Benefit

- An alternative to focusing on harms
- Friedman: there are benefits to be had by working to achieve privacy without minimizing trust; trust can be valuable
  - video (@ 20:03)
- “What happens if we try to construct a society---institutions, organizations, workplaces, schools, families---that primarily use security as a mechanism to protect privacy?”

- **Question:** what are some examples of private environments without security?
- (Also: you’re stuck with trust in the use of privacy technology, as we’ll see next time in more detail)

A division in the reading

- Minimization of disclosure of personal data
- Enforcement of rights when personal data is disclosed
- each has distinctive trade-offs and design challenges

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
  - "Tragedy of the Data Commons"

- Question: How do the costs depend on the details of technology? Consider selective disclosure credentials from the readings. How might what they make possible affect an argument about "inevitable costs" requiring giving up identity information?

A further question about “all or nothing” views of minimization

- Video: Lawsuit to unseal interviews with Saudi men involved in Sept. 11th attacks @ 0:00 - 0:40. FOIA suit requiring statement from Osama Bin Laden @02:10 - 04:00

  Question: When might privacy be a pretext for improperly withholding information? How does this affect legitimate assertions of privacy interest?