24 - Mental models and folk models of security and privacy

Lorrie Cranor

April 16, 2017

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Today!

- Homework 9 is now posted, due May 1
- Midterm 2 on Wednesday
- Mental Models and folk models
- Folk models of home computer security
- Mental models of the Internet
- Folk models of online behavioral advertising

Models

- Mental model
  - The model someone has in their mind about how something works in the real world
  - Used in practice to make decisions
- Folk model
  - “Folk models are mental models that are not necessarily accurate in the real world, thus leading to erroneous decision making, but are shared among similar members of a culture.” (Wash 2010, citing D’Andrade 2005)
  - Note that experts may not necessarily agree on a “correct” mental model

How are these models studied?

- Interviews, surveys, online studies
- Ask participants to describe how something works
- Ask participants to describe their experience, how they made a decision
- Ask participants what is happening, how they would respond to hypothetical scenario
- Ask participants to draw a picture of how something works
- Ask participants to sort (card sorting), compare, select
- Compare responses of experts and non-experts

Folk models of home computer security

Rick Wash, “Folk Models of Home Computer Security” (SOUPS 2010)

- 33 45-minute semi-structured interviews with non-technical home computer users in 3 midwestern cities
- Discussed interviewees’ past security problems or efforts to secure their computers to reveal mental models used to make decisions
- First 23 interviews probed viruses, hackers, data loss, and data exposure (identity theft)
- Last 10 interviews used hypothetical scenarios related to viruses, hackers, and identity theft

Mental models about viruses (malware)

- Viruses are generically 'bad'
  - Underspecified model, viruses are bad, should be avoided
- Viruses are buggy software
  - Associated viruses with bad software, not sure who creates them
- Viruses cause michief
  - Created to annoy people
- Viruses support crime
  - Created to support identity theft and other criminal activities, may not cause noticeable computer problems

How do people with each mental model avoid viruses?

Mental models about viruses (malware)

- Viruses are generically 'bad'
  - Underspecified model, viruses are bad, should be avoided
  - Don’t take specific steps to avoid them
- Viruses are buggy software
  - Associated viruses with bad software, not sure who creates them
  - Avoid by not downloading and executing software you don’t trust
- Viruses cause michief
  - Created to annoy people
  - Avoid by being careful about downloading, where you go online
- Viruses support crime
  - Created to support identity theft and other criminal activities, may not cause noticeable computer problems
  - Detect using AV

Mental models about hackers (anyone who does bad things online)

- Hackers are digital graffiti artists
  - Young, skilled people causing mischief; lack moral restraint; random attacks; harm computers
- Hackers are burglars, criminals
  - Steal info to make money; don't harm computers
- Hackers are criminals who target big fish
  - Work in large groups; target important and rich people to maximize gains
- Hackers are contractors who support criminals
  - Young, skilled people who steal info to sell to criminals; target big companies

How do people with each mental model protect their computer from hackers?

Mental models about hackers (anyone who does bad things online)

- Hackers are digital graffiti artists
  - Young, skilled people causing mischief; lack moral restraint; random attacks; harm computers; don't know how to stop them
- Hackers are burglars, criminals
  - Steal info to make money; don't harm computers; prevent hackers by avoiding some websites, logging out, turning off computer
- Hackers are criminals who target big fish
  - Work in large groups; target important and rich people to maximize gains; not worried because they aren't rich, take basic precautions
- Hackers are contractors who support criminals
  - Young, skilled people who steal info to sell to criminals; target big companies; worried about how companies secure their data

Main takeaways form Wash 2010

- How users perceive threats can affect their security-related behavior
- Users often do not understand threats the same way that sophisticated users do
- Users may take actions that only make sense if you understand their behavior

User mental models of the Internet

Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. SOUPS 2015.

Interview study

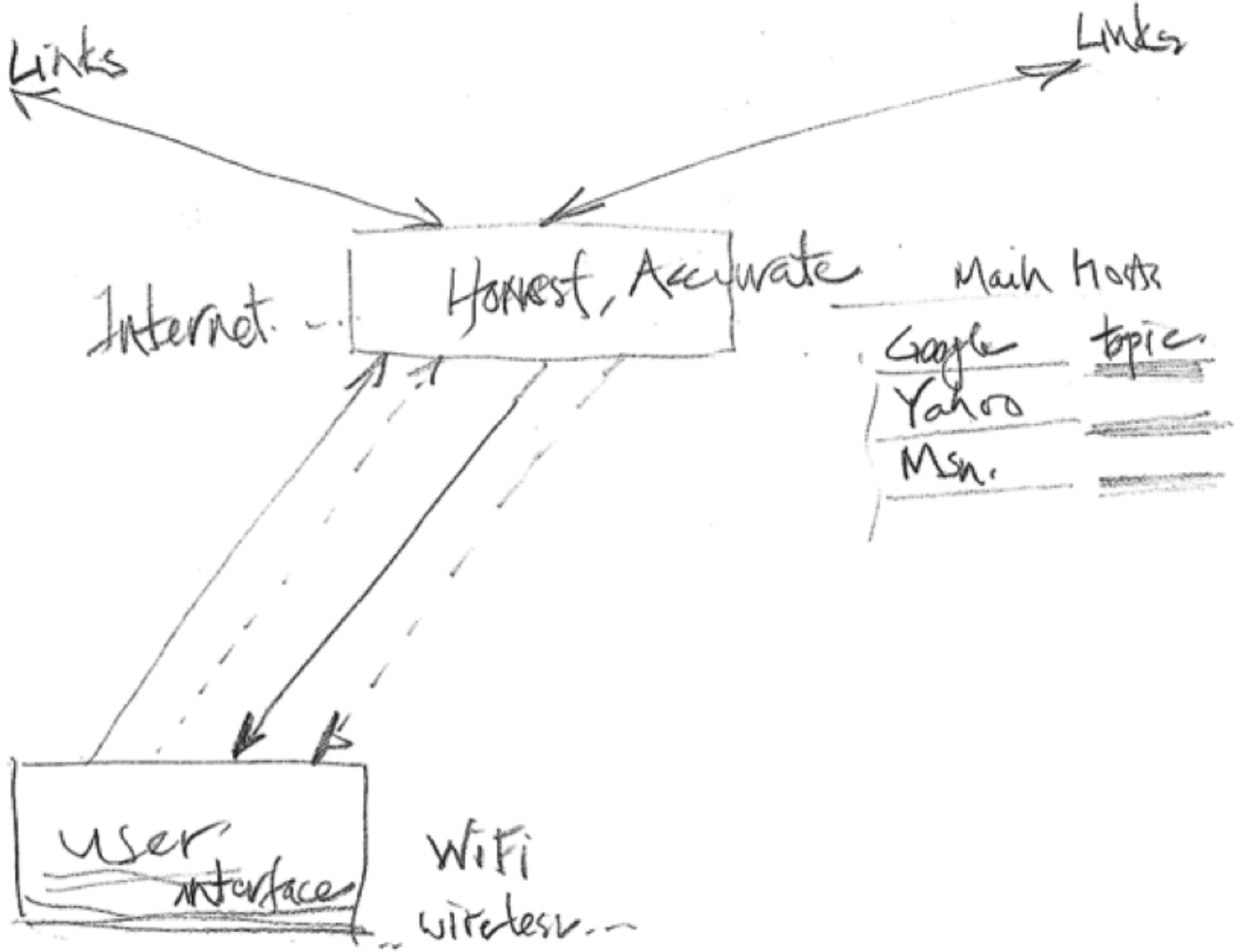
- Semi-structured interviews with 28 technical and non-technical participants
- Asked to make mental model drawings
  - Draw a general diagram of how the Internet works
  - Draw a diagram of where your data goes on the Internet
  - Draw a diagram of specific tasks
    - watching a YouTube video
    - sending an email
    - making a payment online
    - receiving an online advertisement
    - browsing a webpage

Draw a general diagram of how the Internet works

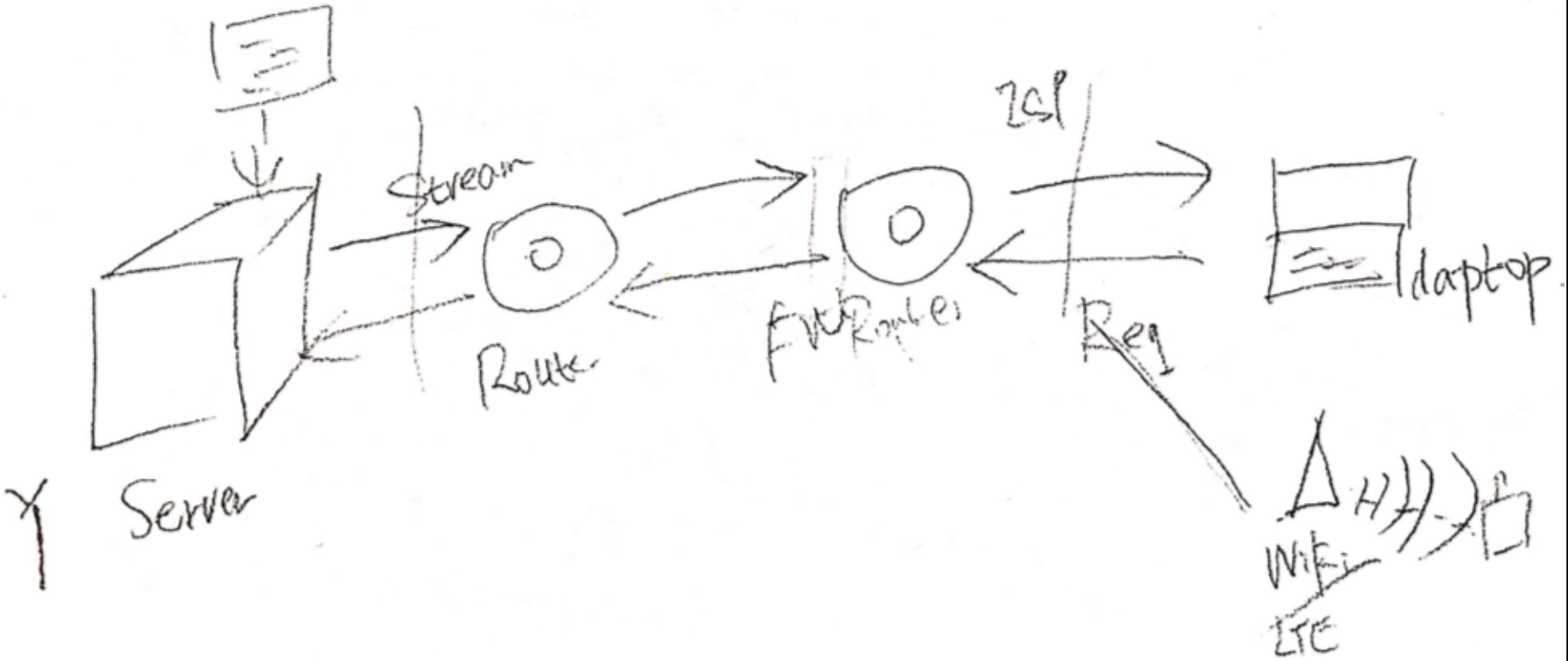
Discuss your diagrams

- Does everyone have the same elements in their diagram?
- What are some important differences between diagrams?

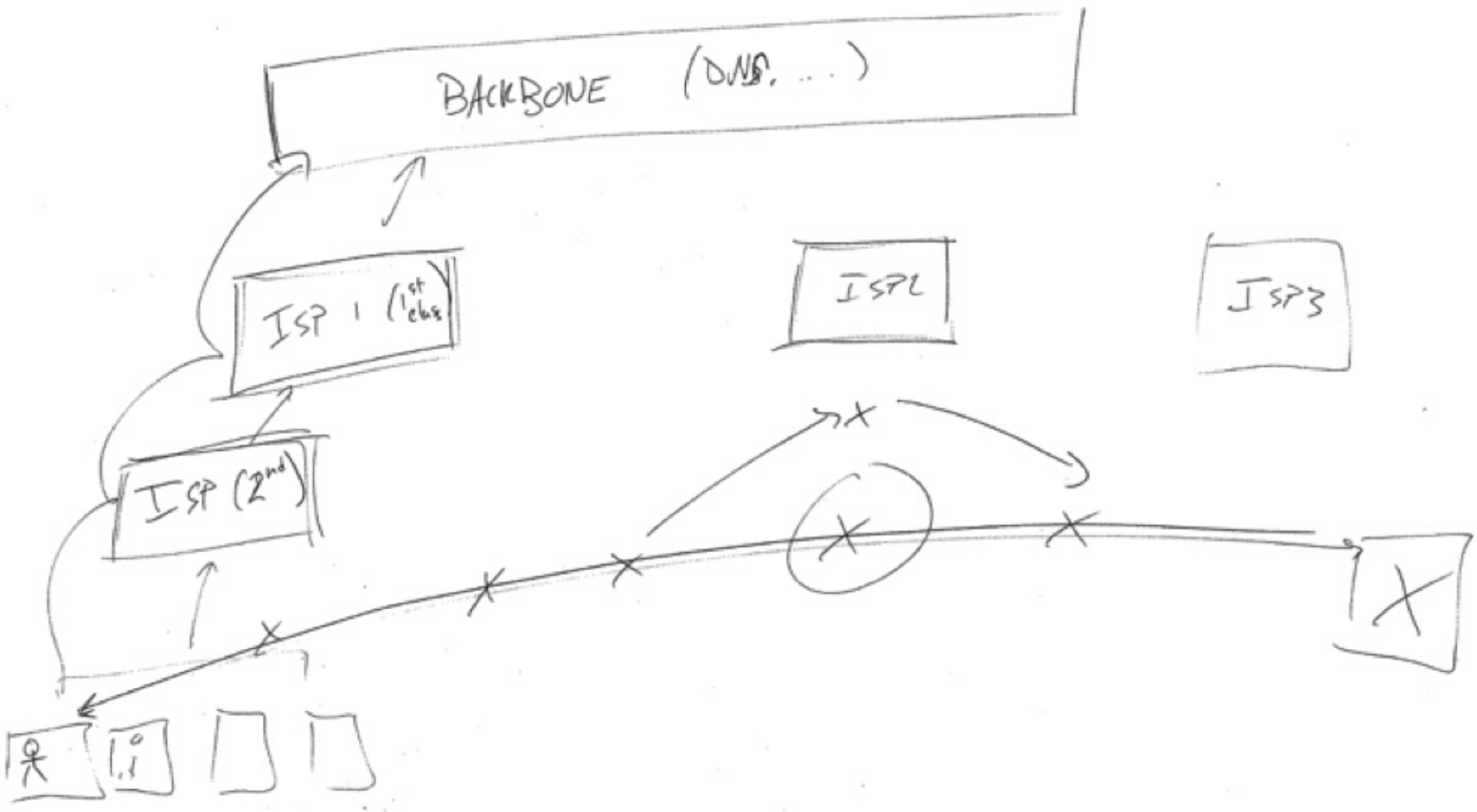
Internet as a service



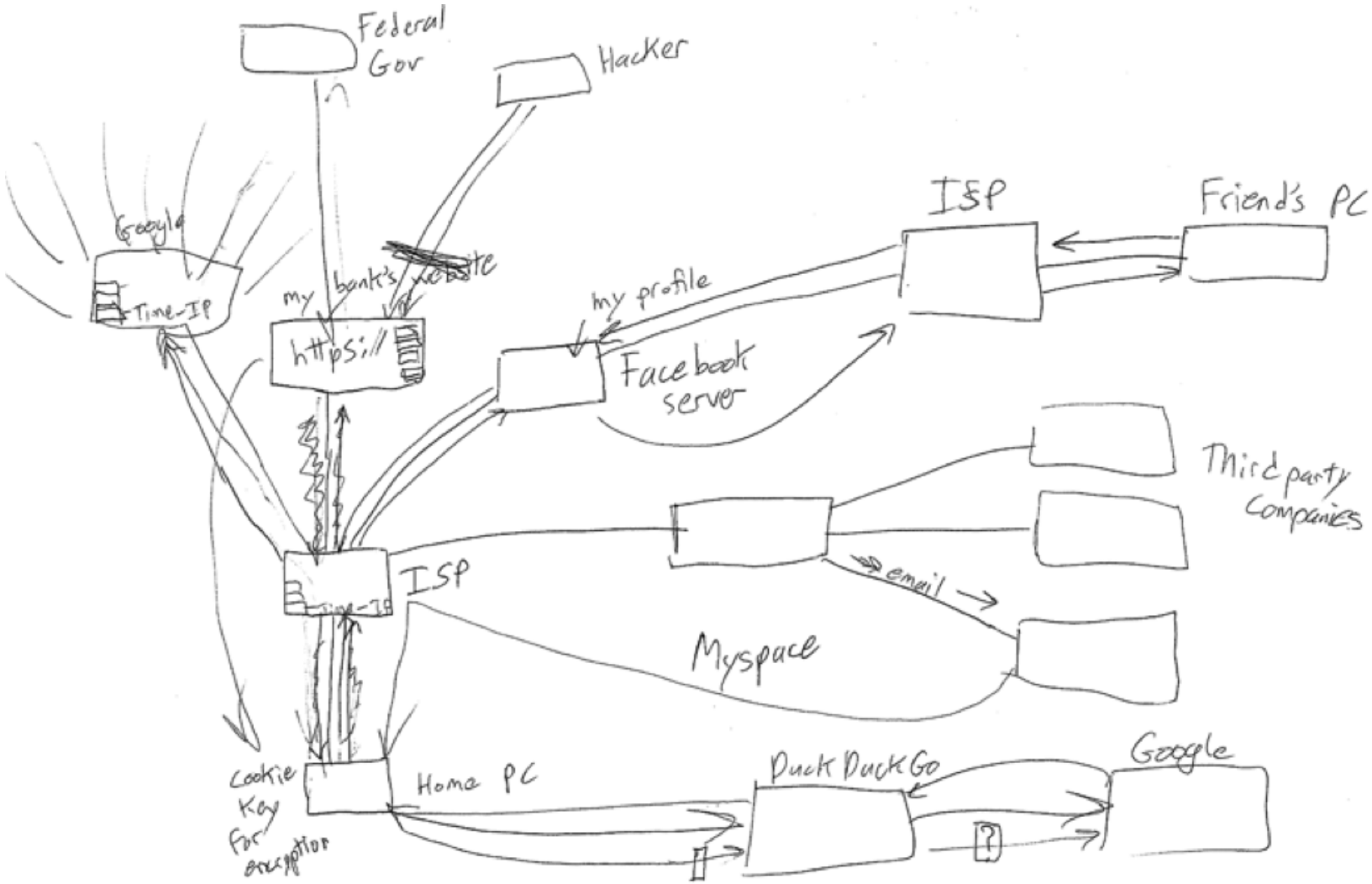
Internet model with hardware components



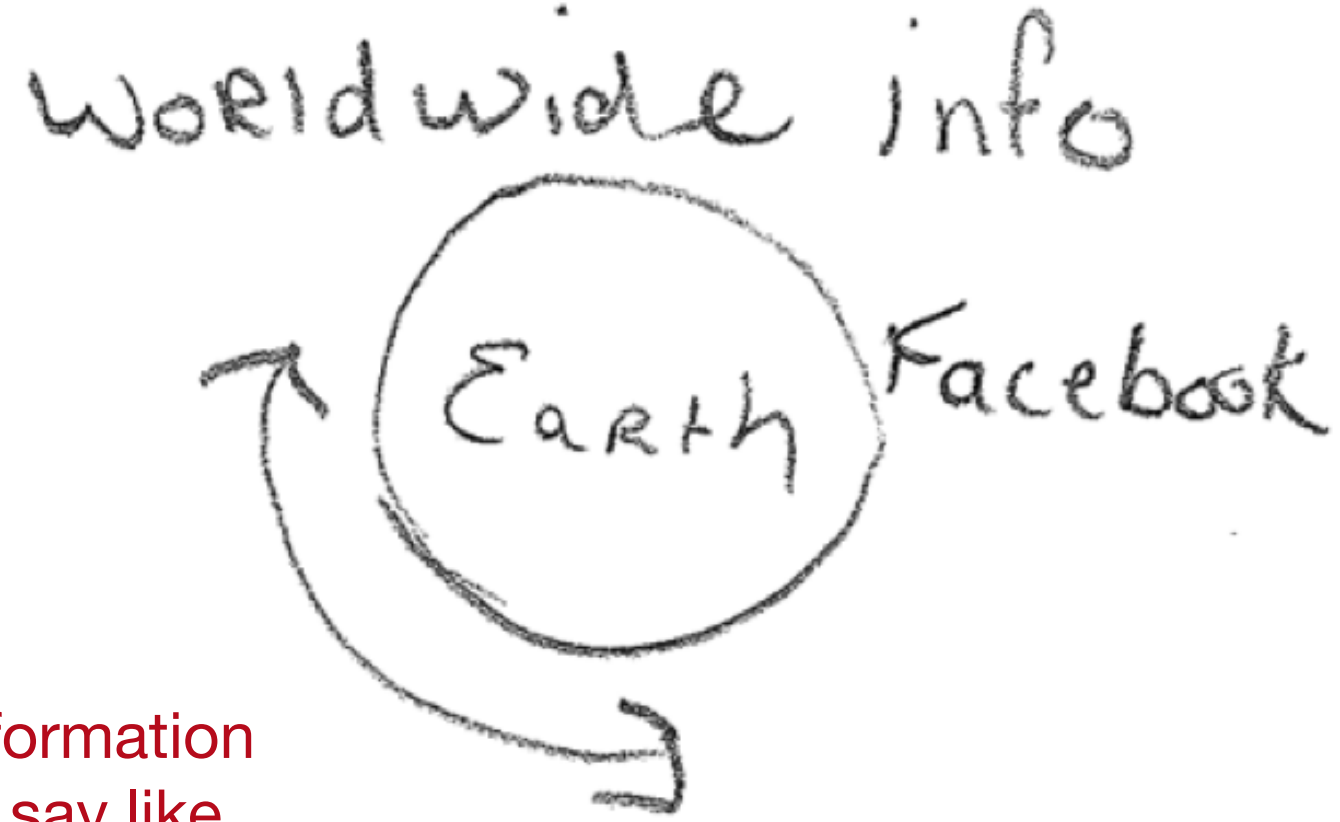
Internet model with multiple network layers



Internet model including who can access information



Where information goes



"I think it goes everywhere. Information just goes, we'll say like the earth. I think everybody has access."

Perceptions of password security

B. Ur, J. Bees, S. Segreti, L. Bauer, N. Christin, and L. F. Cranor. Do users' perceptions of password security match reality? CHI 2016.

Online study

- 165-participant online survey
- 25 pairs of passwords
  - Which is more secure? Why?
- Passwords and password creation strategies
  - Rate security and memorability
- Describe password attackers and how attackers guess passwords

Evaluating password pairs

In your opinion, which of the following passwords is more secure?

punk4life **punkforlife**

punk4life is much more secure	punk4life is more secure	punk4life is slightly more secure	Both passwords are equally secure	punkforlife is slightly more secure	punkforlife is more secure	punkforlife is much more secure
○	○	○	○	○	○	○

Why? *

Rating selected passwords

Please rate the **security** of the following password: **rolltide1** *

1 (very insecure)	2	3	4	5	6	7 (very secure)
○	○	○	○	○	○	○

Please rate the **memorability** of the following password: **rolltide1** *

1 (very hard to remember)	2	3	4	5	6	7 (very easy to remember)
○	○	○	○	○	○	○

Next

Open response questions

- What characteristics make a password easy, hard for an attacker to guess?
- Describe the type of attacker (or multiple types of attackers), if any, whom you worry might try to guess your password
- Explain to the best of your knowledge why an attacker would try to guess your password and how they would do so
- Provide a numerical estimate of how many guesses (by an attacker) would a password need to be able to withstand for you to consider it secure? Why?

Ways People Were Wrong

- Overstated security benefits of:
  - Digits
  - Character substitutions (e.g., a→@)
  - Keyboard patterns (e.g., 1qaz2wsx3edc)
- Did not recognize common words/phrases

Many Ways People Were Right

- Capitalize letters other than the first
- Put digits and symbols in middle, not end
- Use symbols rather than digits
- Avoid:
  - Common first names
  - Words related to account
  - Years and sequences

Perception: How Many Guesses?

- 2 guesses (Min)
- 100,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 guesses (Max)
- 34% ≤ 50 guesses (manual attack)
- **67% ≤ 50,000 guesses (small-scale)**
- 7% ≥ 10^{14} guesses (large-scale)

Folk models of online behavioral advertising

Yaxing Yao, Davide Lo Re, and Yang Wang. 2017. Folk Models of Online Behavioral Advertising. *2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '17), 1957-1969. DOI: https://doi.org/10.1145/2998181.2998316

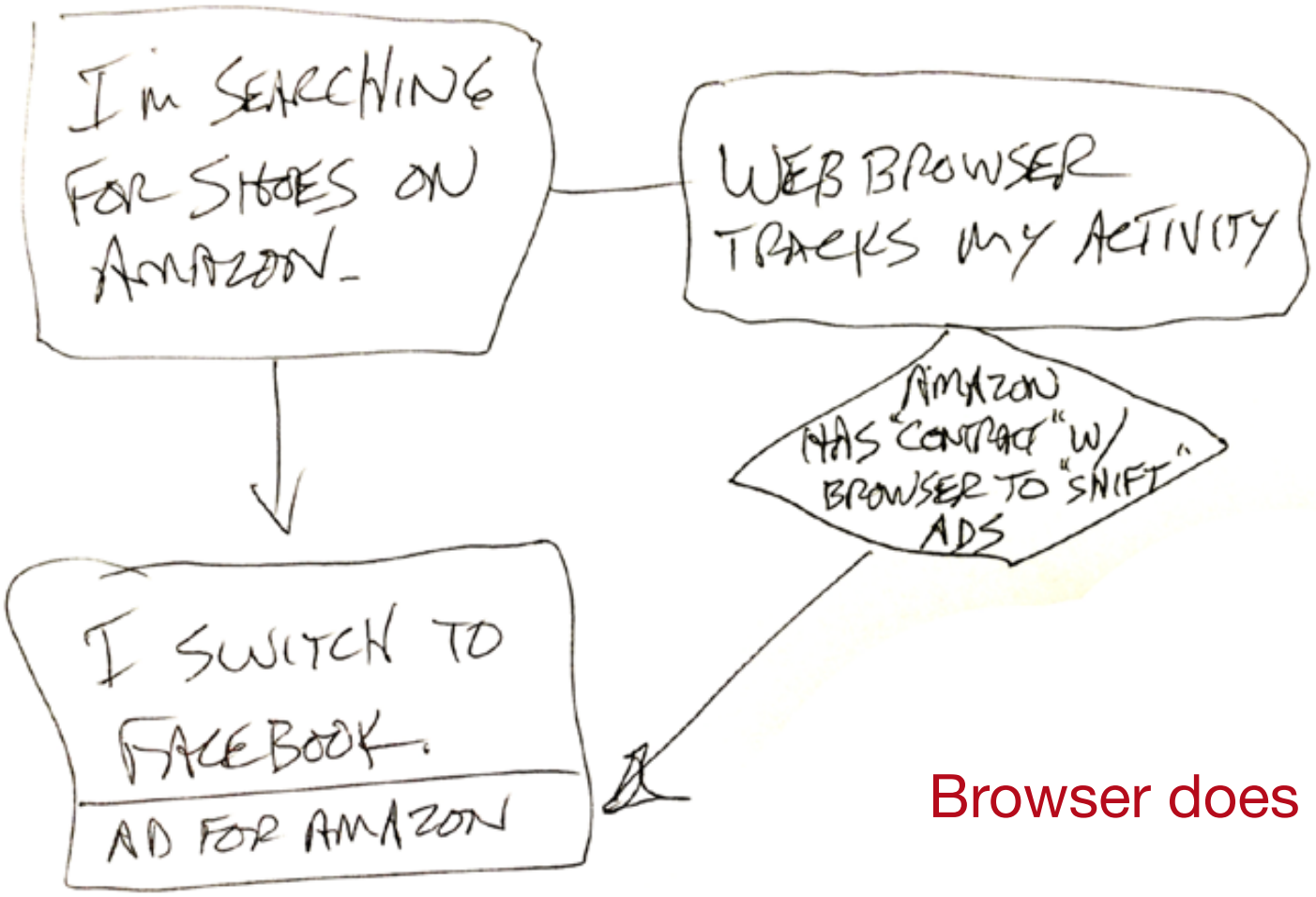
Interview study

- 21 participants
- Interviews discussed
  - How OBA works
  - Privacy tools
- Drawing pictures based on hypothetical scenarios

Hypothetical scenario

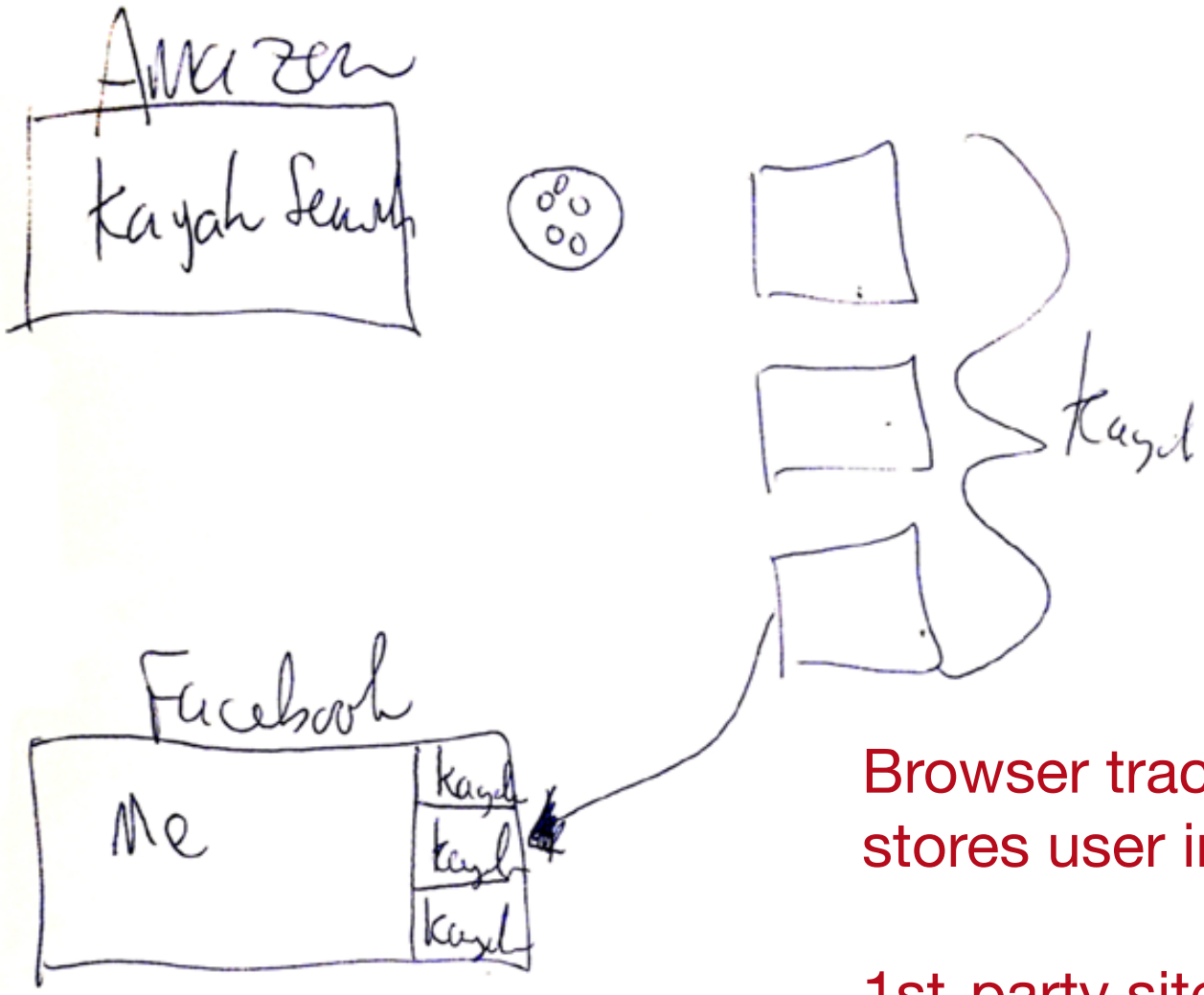
- You first look for shoes on Amazon.com and a few hours later you visit Facebook and see other shoe ads there
- How would you draw the information flows that make this happen?

Browser-pull



Browser does it all

1st-party pull



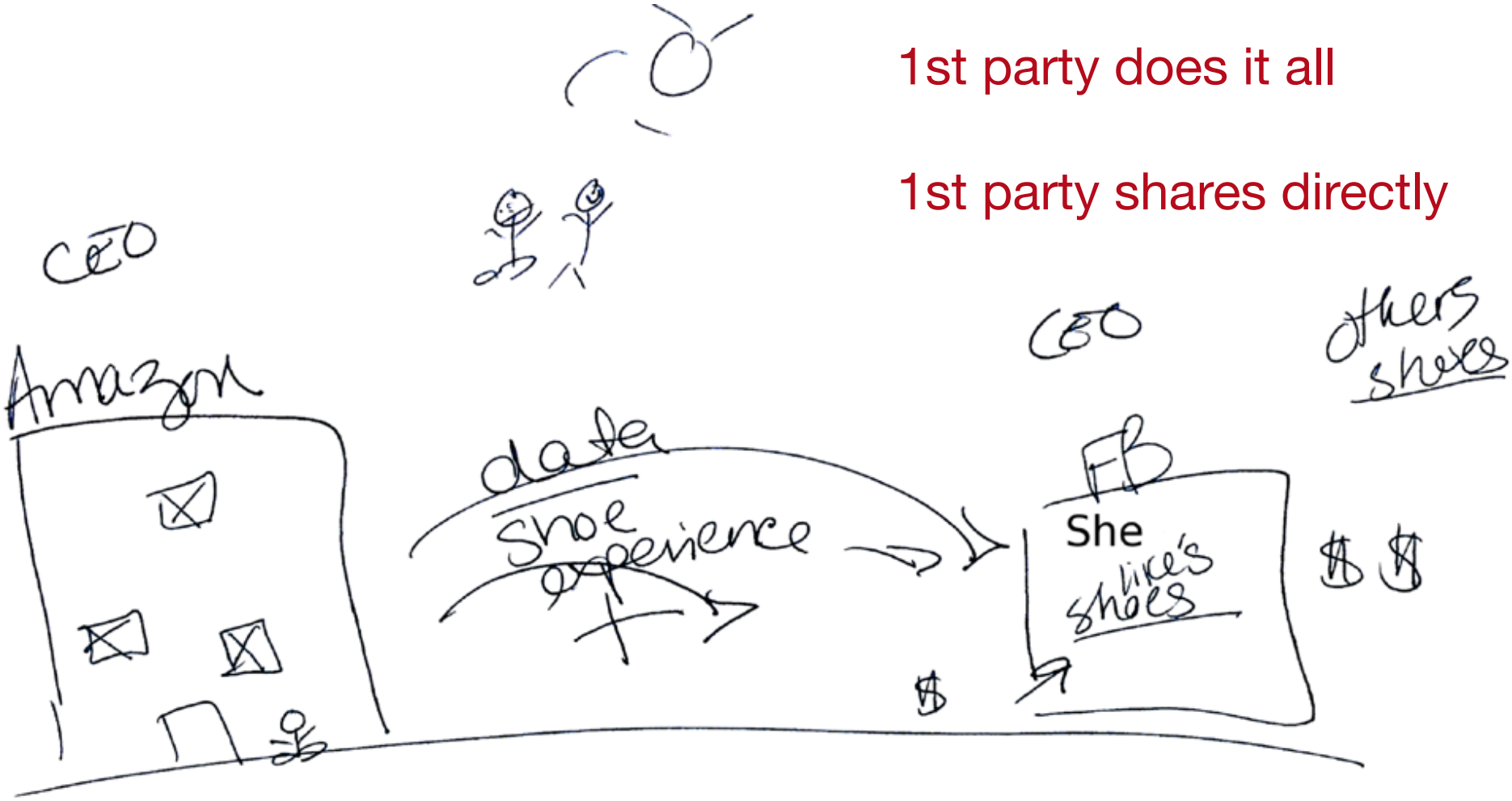
Browser tracks and stores user info

1st-party sites pull ads

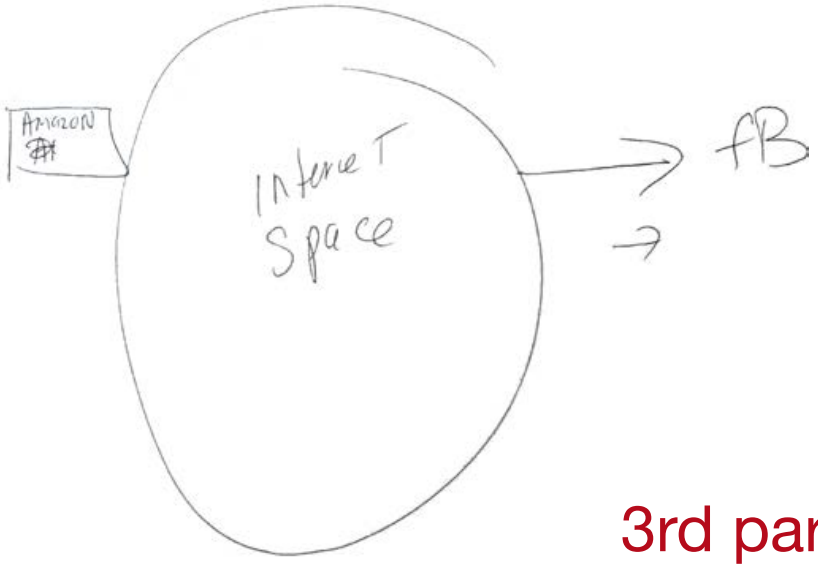
Connected 1st party

1st party does it all

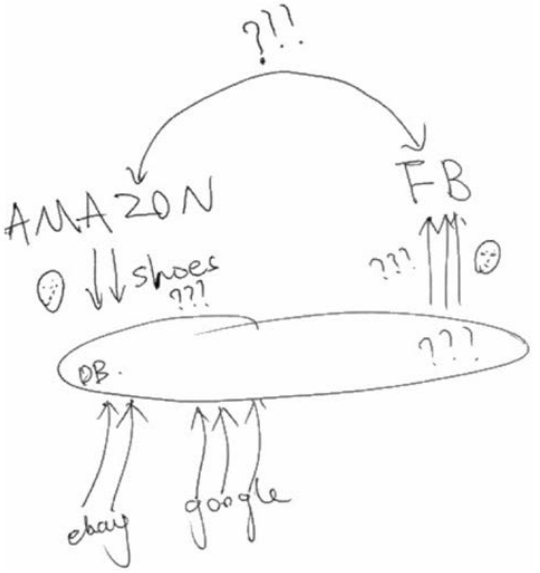
1st party shares directly



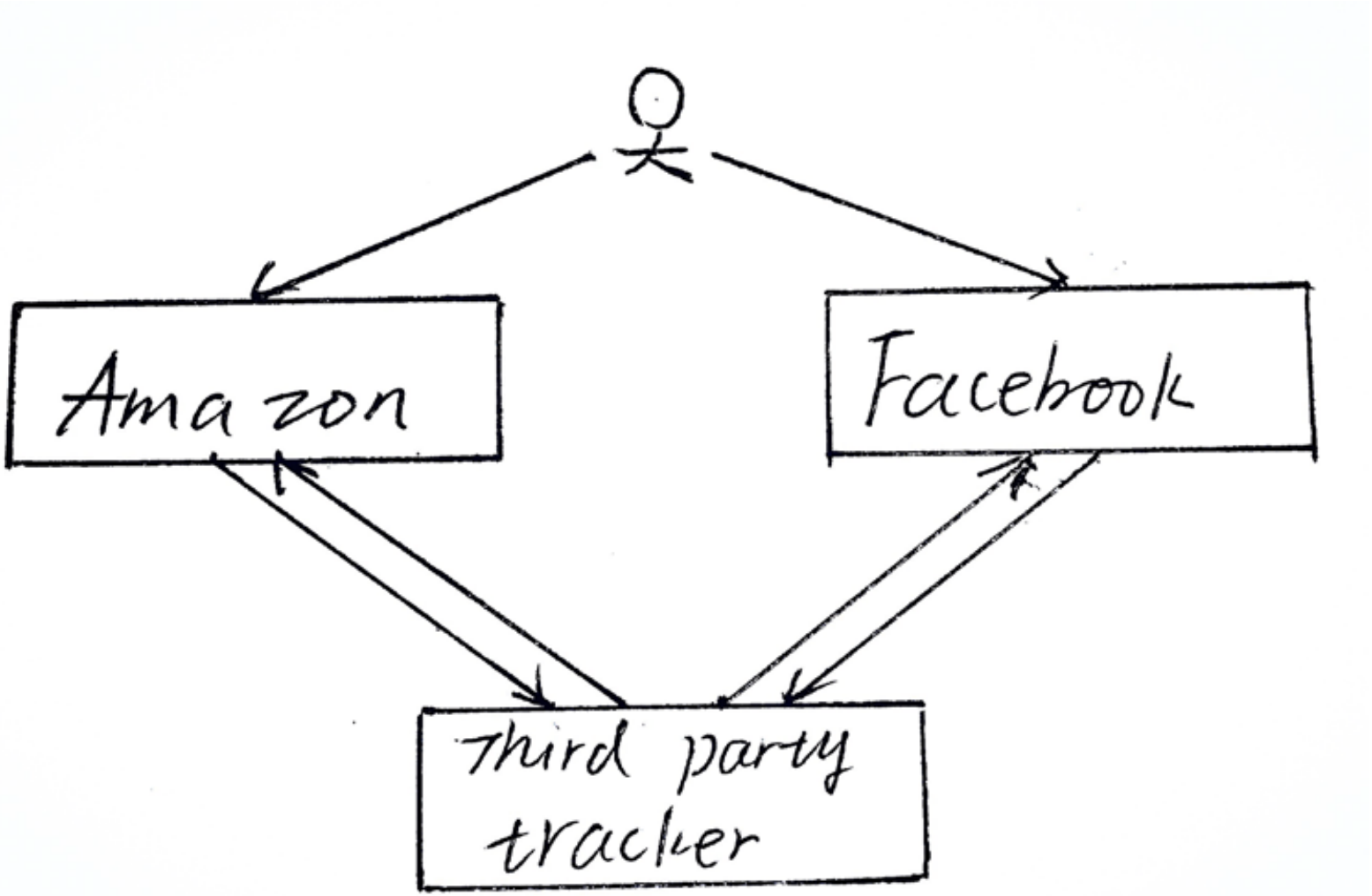
3rd party



3rd party does it all



Common practice



What are the implications of these mental models for opt-out tools?