


# Reifying Privacy in Software and Hardware: Defining What We Want to Protect

James Mickens  
Harvard University



# What Is Privacy?

**privacy** **noun**

pri·va·cy | \ 'prī-və-sē , especially British 'pri-\  
plural **privacies**

## Definition of *privacy*

- 1 **a** : the quality or state of being apart from company or observation : SECLUSION
- b** : freedom from unauthorized intrusion



*Literally*

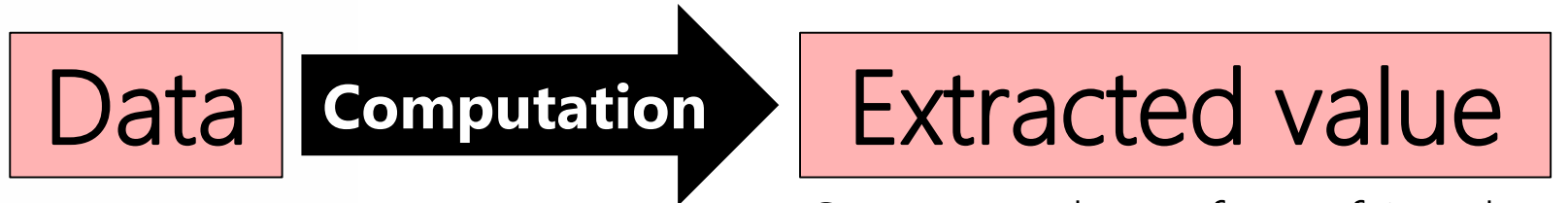
^

# What Is Privacy?

: the quality or state of being apart from company or observation : SECLUSION

?

Computation is observation!



- Status updates from friends
- Recommendations for books, movies, songs, news articles
- Highly-available data storage for emails, documents, code
- E-commerce



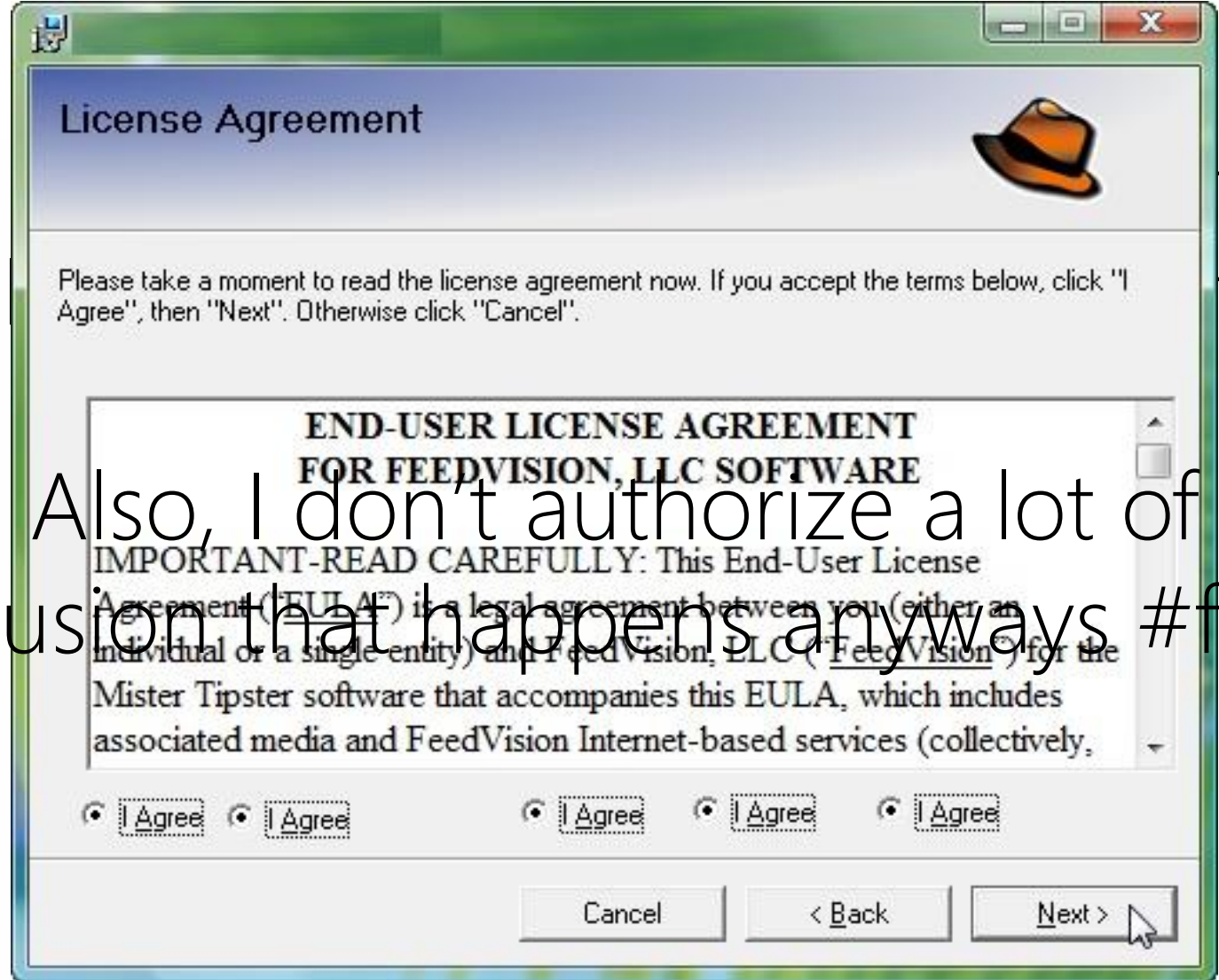
*Literally*

^

# What Is Privacy?

?

Also, I don't authorize a lot of intrusion that happens anyways #fml<sup>2</sup>



on

ml

#fml<sup>2</sup>



## Facebook Rebuked for Failing to Disclose Data-Sharing Deals

# Popular Weather App Collects Too Much User Data, Security Experts Say

## How to Stop Seeing Awkward Tinder Dates on LinkedIn

61 COMMENTS



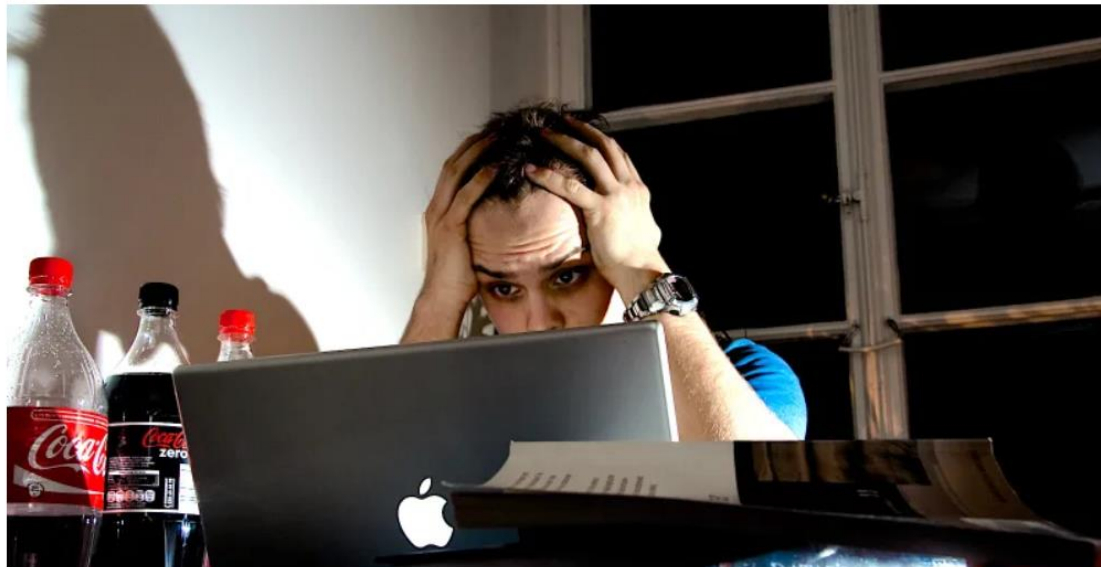
Patrick Allan

3/21/18 3:30pm • Filed to: PRIVACY ▾

59.6K

27

2



A sign outside Facebook's headquarters in Menlo Park, Calif., after a New York Times article revealed details of the company's data-sharing deals. (Elijah Nouvelage/Reuters)

By Michael LaForgia, Nicholas Confessore

Dec. 19, 2018

Facebook and some of the other major social media companies faced sharp criticism on Wednesday after a New York Times article revealed details of the social network's data-sharing deals.

A Chinese tech conglomerate has been attempting to install its smartphones around the world and attempting to gain user permission, according to a London-based security firm.

The firm, "Accurate Radar," collects data on users, including names, email addresses and unique 15-digit identification numbers on TCL servers in China, according to the firm. The firm also found the app "Weather—Simple weather forecast."

The amount of data the app collects.

Share

Tweet

Privacy

Ads

## Profile visibility off LinkedIn

Choose how your profile appears via partners' and other permitted services

Should we show information from your profile to users of permitted services such as Outlook? [Learn more](#)

Yes



Weasel set of ill-defined cardinality and membership



## Privacy

### Profile visibility off LinkedIn

Choose how your profile appears via part

Should we show information from  
such as Outlook? [Learn more](#)

Yes ☒

Potentially every  
online service that  
has existed or will  
ever exist



## Off-LinkedIn Visibility

Two of LinkedIn's goals are to help members be found for opportunities and to facilitate better informed professional communications, both on and off the site. For example, **public profiles** can be found through search engines. In addition, users of certain mail or calendar services may also see in those services "mini" profiles of members they interact with.

You may prefer to limit the visibility of your profile information outside of LinkedIn. Below are two settings that enable you to do that.

### › Public profile

### ✓ Other services (formerly "third party applications"), excluding search engines

Through our partnerships and developer program, we enable certain affiliates, partners, customers, and other permitted developers to display to their users information from the profiles of members they meet, write to or about, manage or consider for talent or other opportunities, take social actions (e.g. follow their company), etc. Some examples include Outlook and **Yahoo Mail**, Calendar or Contacts, Apple and **Samsung** native mail, contacts and calendar phone apps, **Cortana**, **Evernote**, social media aggregators (e.g. tools for **company brand administrators** to consolidate interactions with followers across social media), talent and lead managers.

You can opt out using this [setting](#) (formerly known as "sharing data with third parties").



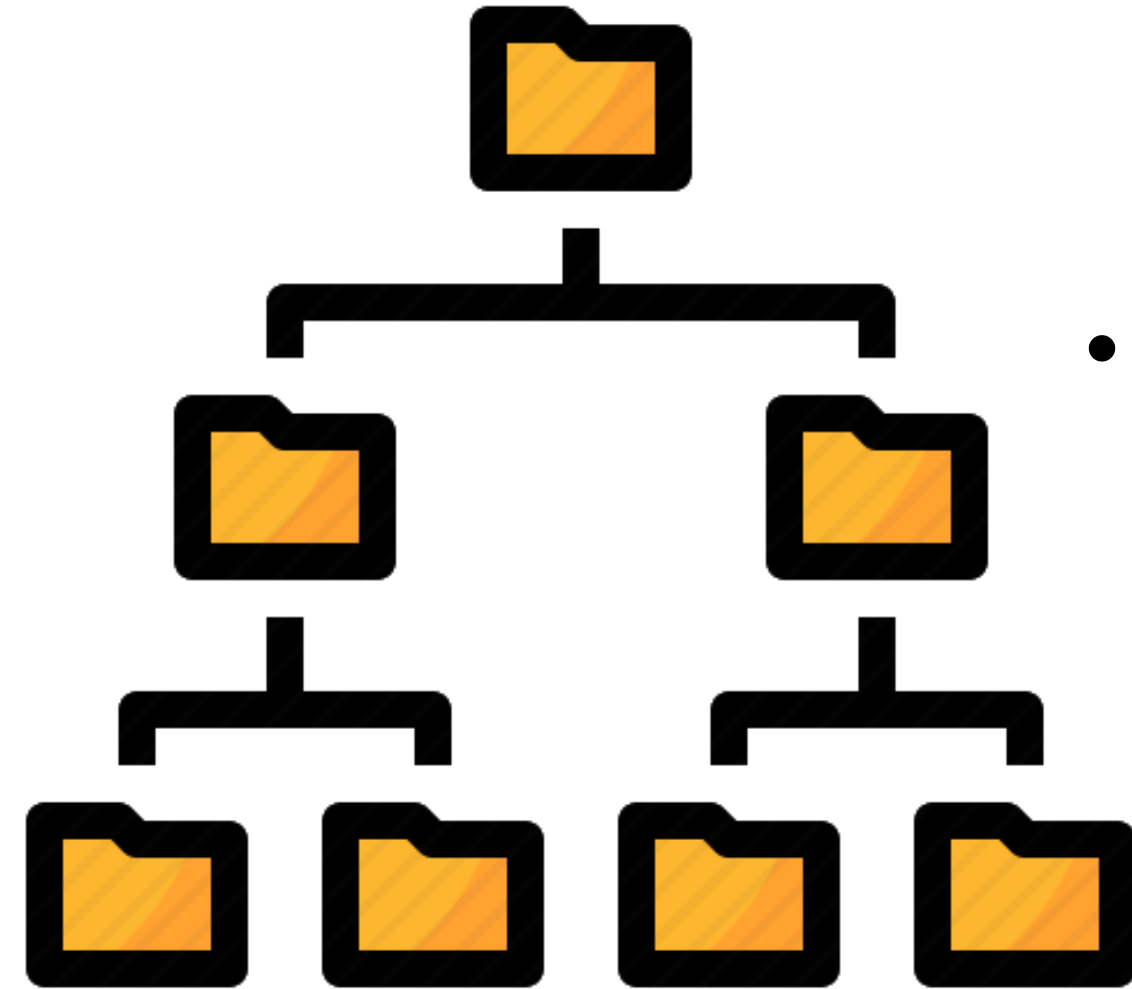
**“How Do We Free Ourselves  
Of This Existential Fear  
About How Our Data  
Is Being Used?”**

Jean Paul Sartre  
1946





# Storage As A Visual Metaphor

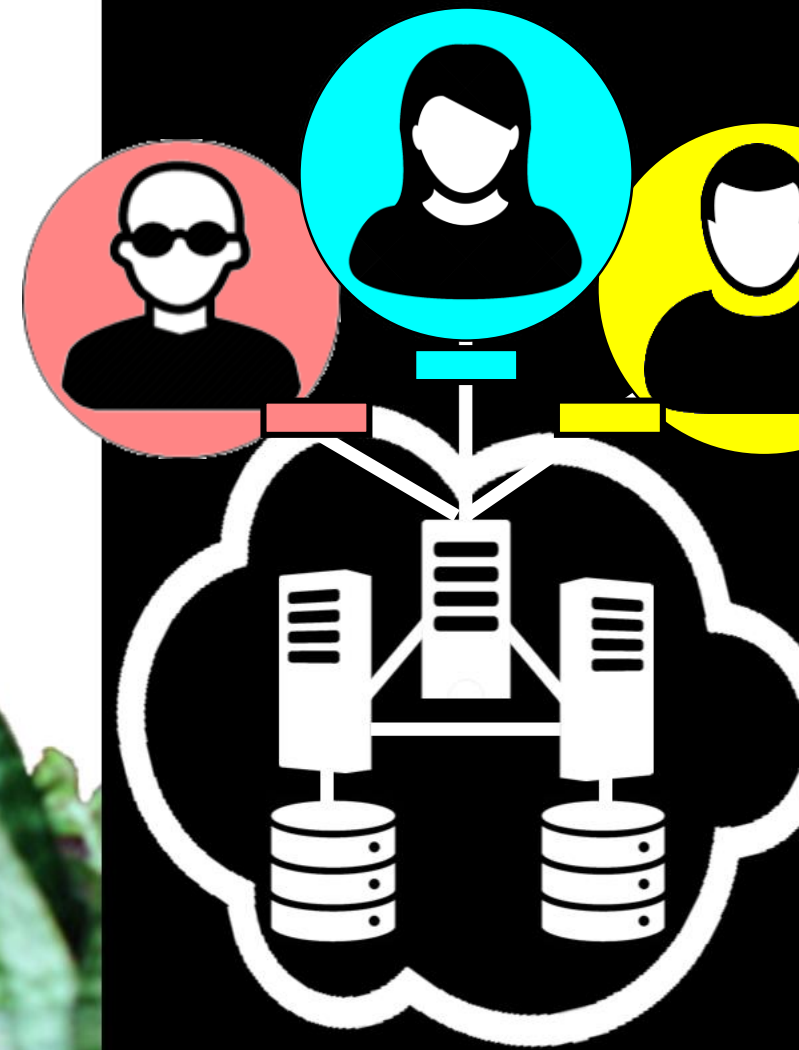


- The tree metaphor helps **users** as well as **developers** to organize information
- The tree metaphor enables **specific questions**
  - Where does a particular file live?
  - What are the relationships between different files?
  - Who should be able to access a particular set of files?



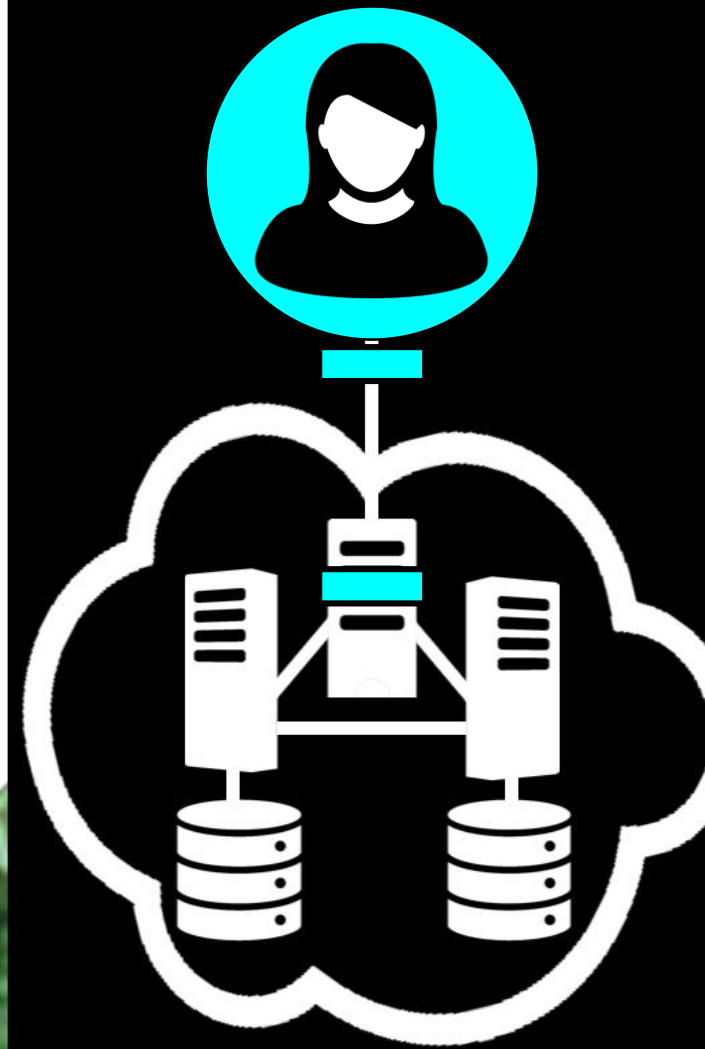
# What Is The Visual Metaphor For Data Privacy?

# Aggregation



**Aggregation**

**Derived data flows**

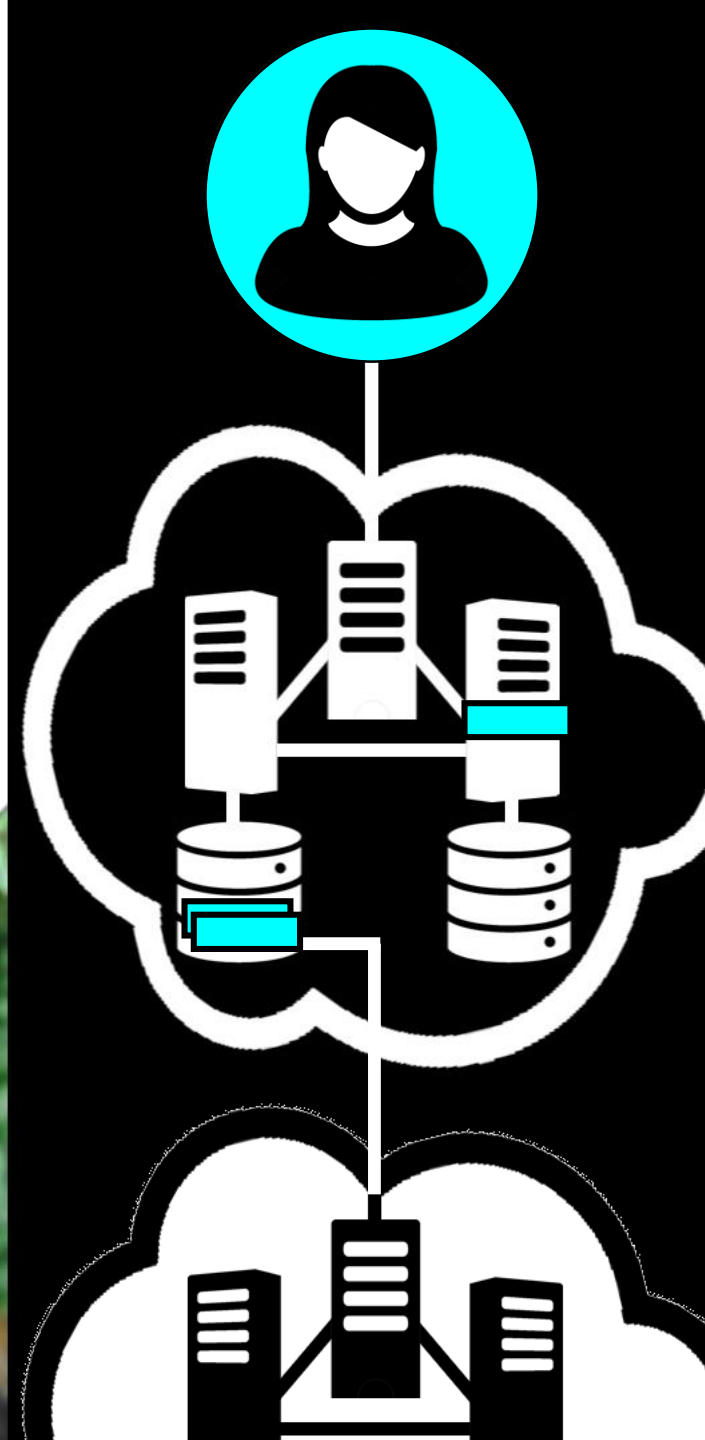




**Aggregation**

**Derived data flows**

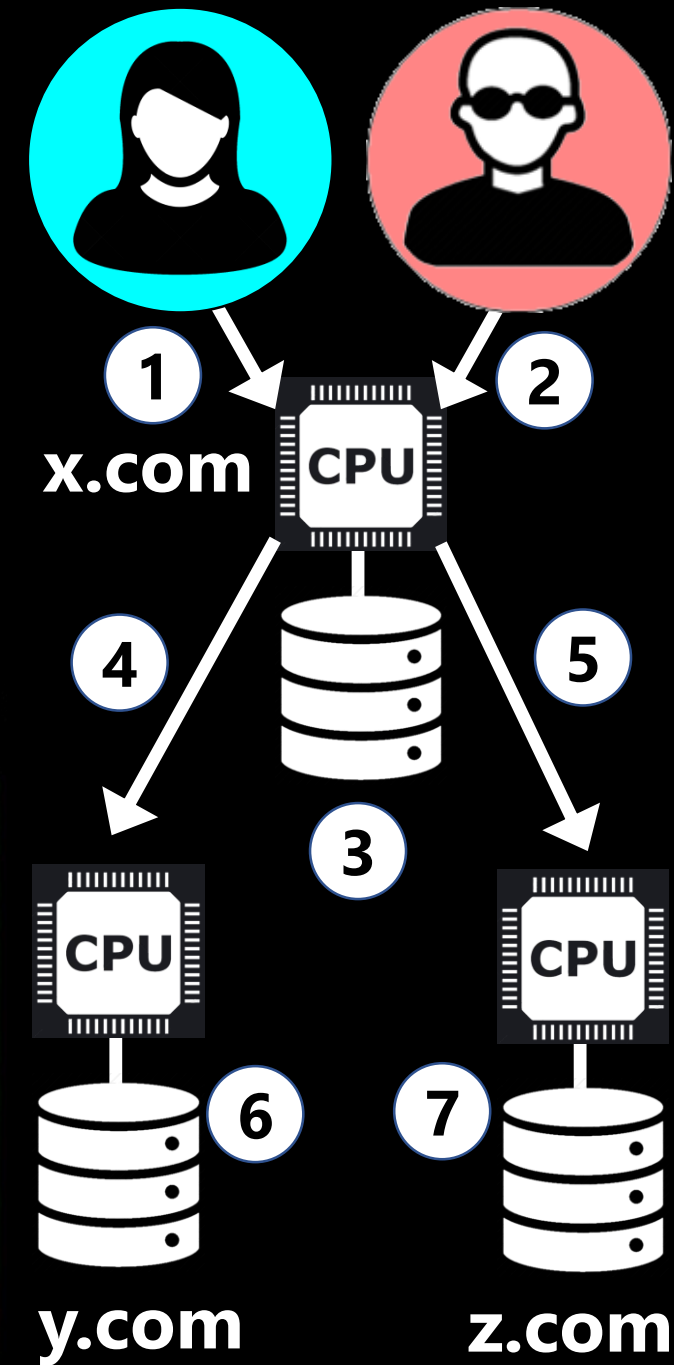
**Third-party sharing**



# Data Flow Graphs as a Visual Metaphor For Privacy

1. Can x.com see my data?
2. Is x.com allowed to aggregate my data with the data of other users?
3. Can x.com persistently store my data?
4. Can x.com send my data to y.com?
5. Can x.com send my data to z.com?
6. Can y.com persistently store my data?
7. Can z.com persistently store my data?

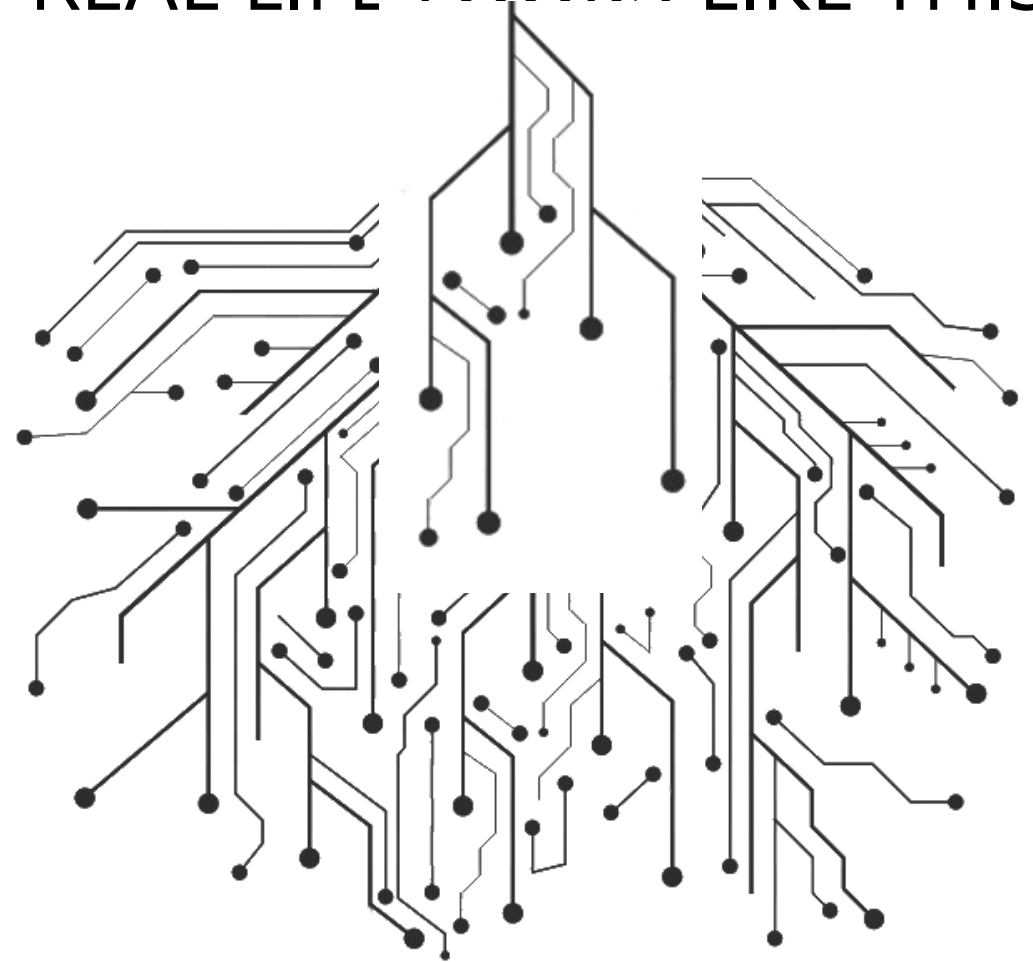
**Data flows should be denied by default—force online services to explicitly enumerate and declare them!**



# Code, EULAs, and Law as Graphs

- Hardware designers and software developers make data flows an engineering building block
- EULAs are expressed as graphs
  - Validation for “privacy acceptability” can be (partially) automated
  - Violations are now cleanly defined
- Privacy legislation can use the language of data flows

REAL LIFE LOOKS LIKE THIS



BUT AT LEAST WE SEE IT