

Beyond Code: Ethical Data Privacy in Computing

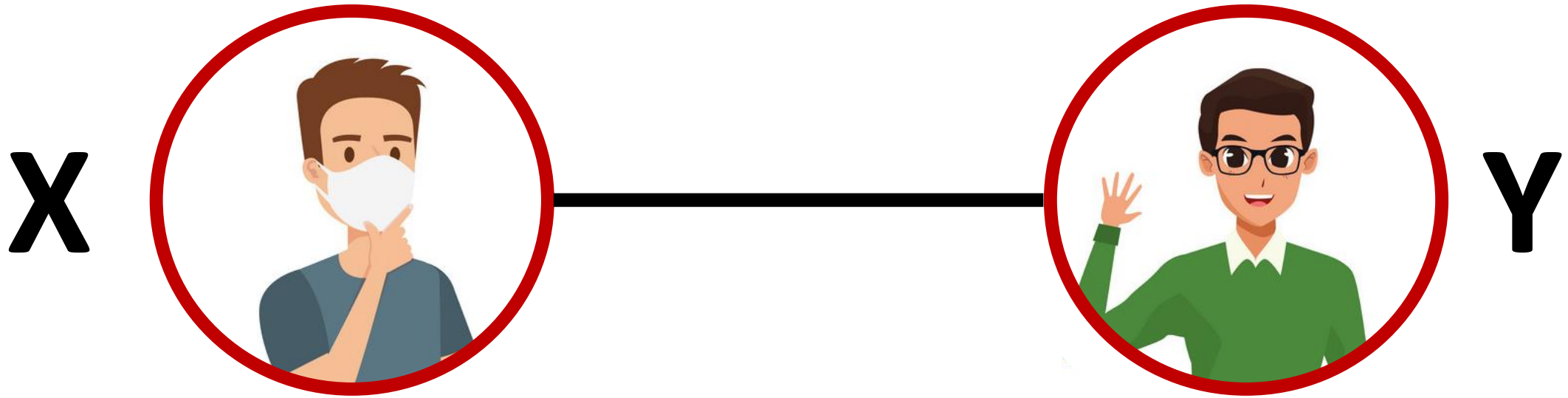
Maryam Majedi

majedi@ucsb.edu

27 November 2023



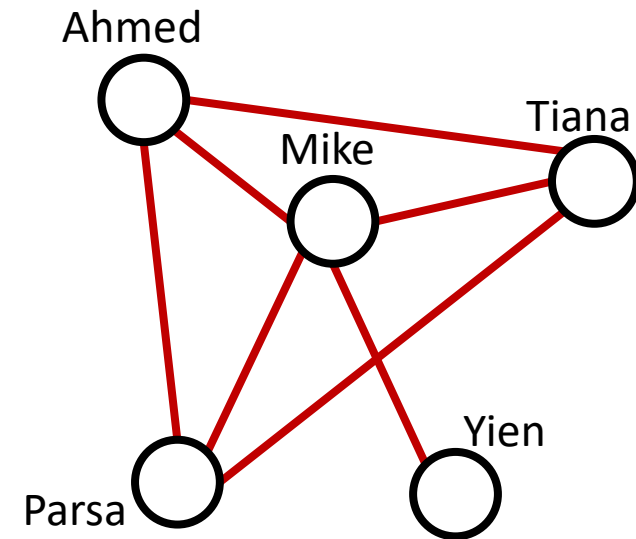
“Contact tracing is the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission.”



Node: Person
Edge: Contact

→ Within proximity at approximately the same time.

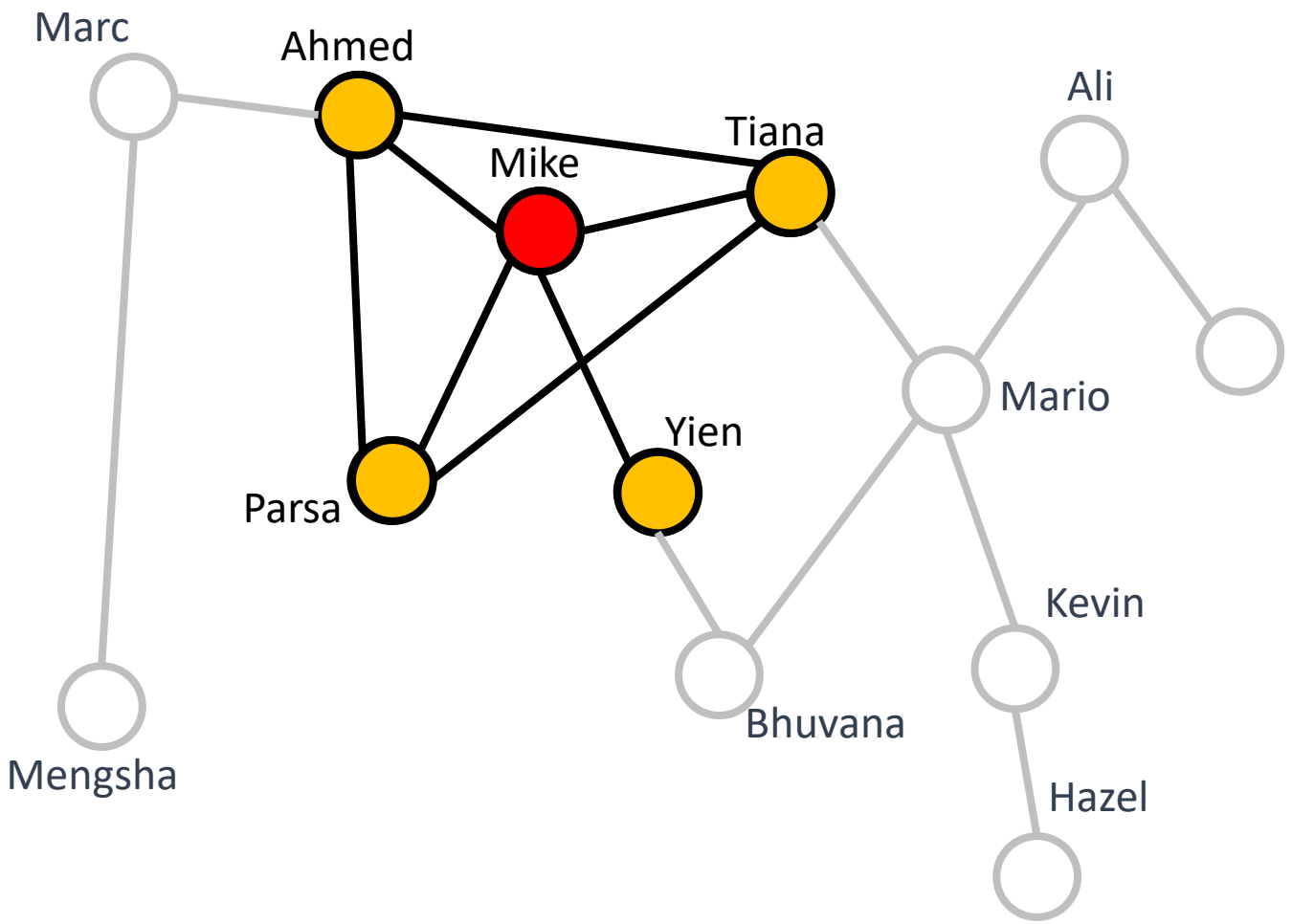
Name	Location	Arrival Time	Leaving Time
Mike	A	Feb 14th, 9:12 PM	Feb 15th, 1:35 AM
Parsa	A	Feb 14th, 9:37 PM	Feb 15th, 1:15 AM
Tiana	A	Feb 14th, 10:06 PM	Feb 15th, 1:35 AM
Mike	B	Feb 14th, 1:57 AM	Feb 15th, 7:30 AM
Tiana	B	Feb 14th, 1:57 AM	Feb 15th, 9:30 AM
Ahmed	A	Feb 14th, 6:08 PM	Feb 15th, 8:30 AM
Mike	C	Feb 15th, 8:00 AM	Feb 15th, 4:00 PM
Yien	C	Feb 15th, 8:30 AM	Feb 15th, 4:30 PM





A **close contact** in the context of COVID-19 is defined by the CDC to be

“Someone who was within 6 feet of an infected person for a cumulative total of 15 minutes or more over a 24-hour period starting from 2 days before illness onset.”

- Centers for Disease Control and Prevention (CDC)



-  Confirmed case
-  Close contact

Empowering your system

- How can we make this system more powerful?
- Examples?
 - Ability to prioritize people who are at risk .
 - Ability to prioritize health care workers.
 - Provide more in-depth analysis for future research.
 - ...
- We need more data!
 - Age, health profile, vaccination history, etc.

Identifying gatherings

Identifying hot spot zones
or large crowd gather, and
where social distancing is
not observed

Infected areas

Identifying areas frequented by more COVID-19



Identifying super spreaders

- Identifying people who travelled and thus are potential super spreaders to prioritize for rapid testing



Activity 1

- On the Worksheet
 - Review the provided table of data
 - Answer the questions
 - Try to make more guesses about our characters



Some possible implications

Name	Location	Start Time	End Time
Mike	A	Feb 14th, 9:12 PM	Feb 15th, 1:35 AM
Parsa	A	Feb 14th, 9:37 PM	Feb 15th, 1:15 AM
Tiana	A	Feb 14th, 10:06 PM	Feb 15th, 1:35 AM
Mike	B	Feb 14th, 1:57 AM	Feb 15th, 7:30 AM
Tiana	B	Feb 14th, 1:57 AM	Feb 15th, 9:30 AM
Ahmed	A	Feb 14th, 6:08 PM	Feb 15th, 8:30 AM
Mike	C	Feb 15th, 8:00 AM	Feb 15th, 4:00 PM
Yien	C	Feb 15th, 8:30 AM	Feb 15th, 4:30 PM

- B is Mike's home
- C is Mike's work
- Mike attended a gathering with Ahmed, Tiana, and Parsa
- A is Ahmed's home
- Ahmed was the host
- B is Tiana's home
- Tiana may be Mike's partner
- ...

→ Given the distance between locations, we might guess how a person commutes

They were doing the weekly quizzes 

Either he works too much or parties too much

Mike and his friends are irresponsible 

Mike has a day time job

Mike is probably into Tiana 

Mike is social, he meets other people a lot 

Ahmed throws some good parties 



Who Needs Privacy?



- Privacy can clearly be valuable for those who have done wrong
- But is it true that the innocent have nothing to hide?

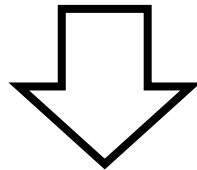
Who Needs Privacy?

- Sometimes we need privacy to protect ourselves
- Ex: Identity theft, but also those fleeing domestic abuse

Image source:
uslegalservices.n
et



- We might also worry about the government having access to the information--even if it's gathered with the best of intentions, it could be misused in the future



- And the same is true of private companies having access to the data



**BIG BROTHER IS
WATCHING YOU**

Who Needs Privacy?

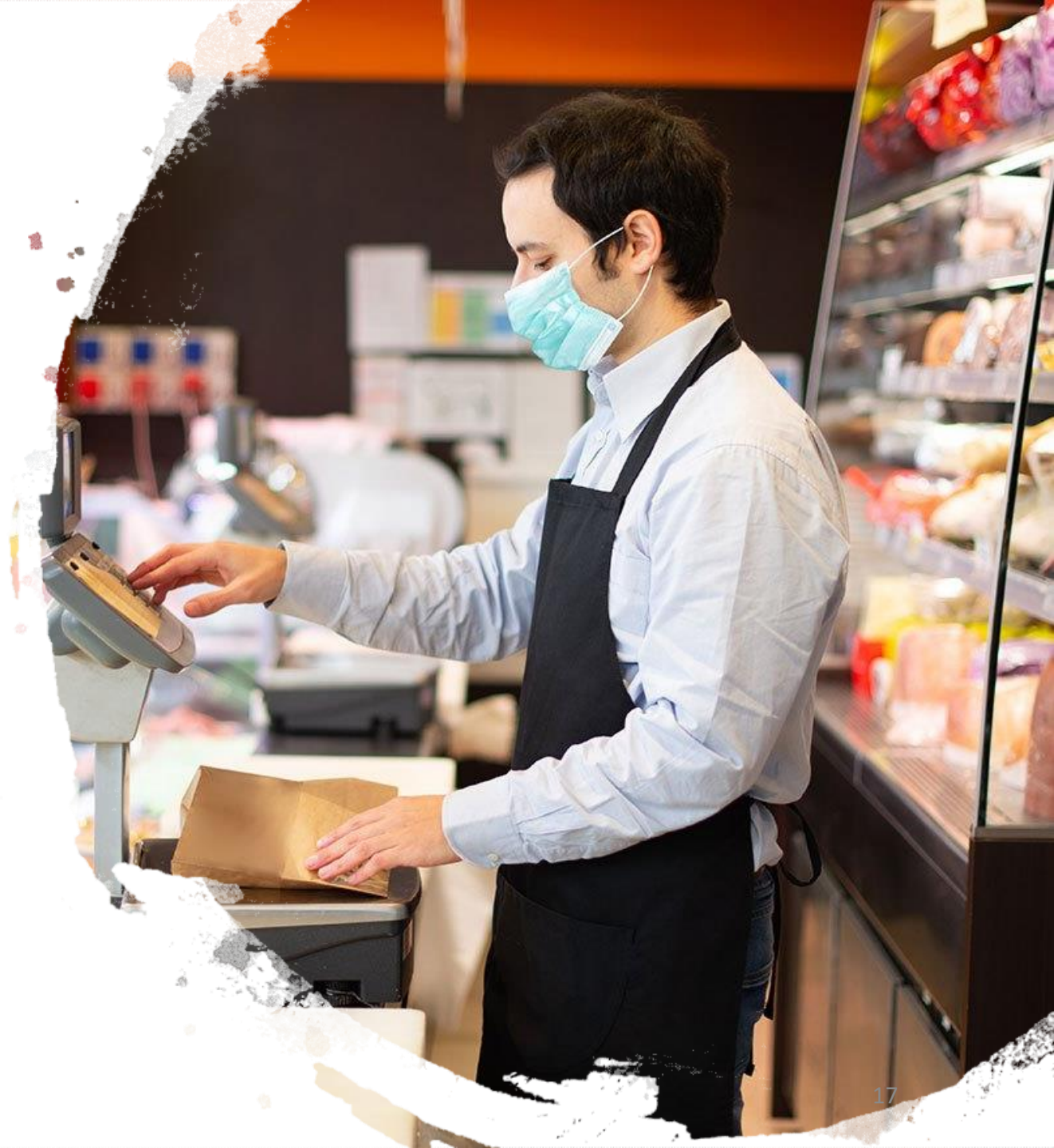
- Sometimes we need privacy in order to present different faces to different people
- Sometimes to avoid discrimination, and sometimes just to maintain boundaries

Image source:
superhero hype.c
om



Isaac: A grocery store worker

- Isaac is a grocery store worker who has a chronic illness. He worries that if his employer finds out he is high risk, he will be assigned fewer shifts or suffer stigma at work.



Privacy is all about
controlling access to
information

But

some of this same
information might
help us improve
quality of life



Addressing the ethical issues

- Could we have collected less or different information and still accomplished the task of contact tracing?
- How could we have changed what information we collect to minimize the potential for inference of further information?



Exposure notification system



Image source:
[washingtonpost.com](https://www.washingtonpost.com)

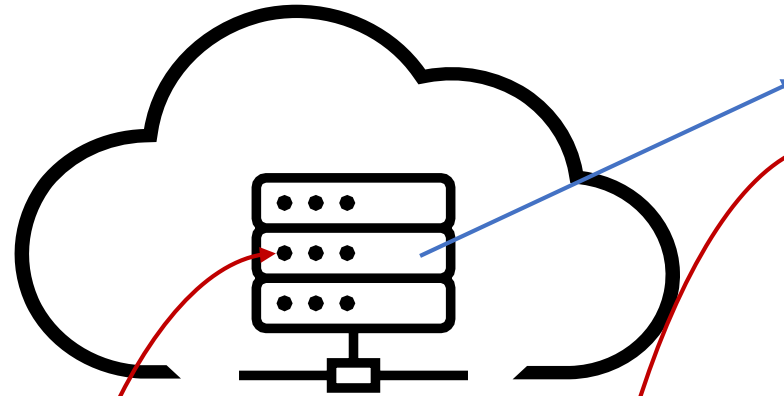
Exposure notification system

Key	Time
K001	t1
K284	t4
K112	t3
K390	t4
K222	

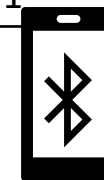
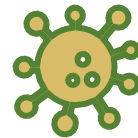
K444	t5
------	----

K222	t5
------	----

Key	Time
K831	T6
K426	T1



Key	Contact info
K001	647.888.1111 ⓘ
K284	647.222.3333 ⓘ
K112	647.111.4563 ⓘ
K390	647.555.6666 ⓘ
K222	647.222.4444 ⓘ
K831	647.333.9999
K426	647.999.8888
K444	647.000.6666



Limited Collection

We collected:

- Demographic information
- Location
- arrival and departure times

Purpose: Notify individuals who have been in a proximity to a confirmed case during the past two weeks.

Therefore we need:

- Proximity records for the last 14 days
- A way to notify

Retention

Limiting Use, Disclosure, and Retention

- “... Personal information shall be retained only if necessary, for the fulfillment of those purposes.”

Old

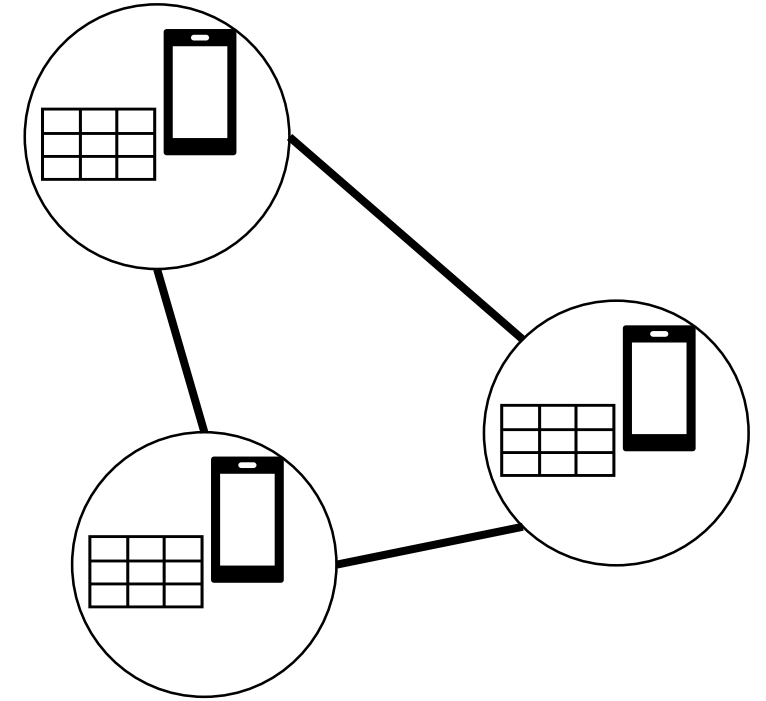
Key	Time
K222	t5

Exposure notification system

- Limited collection compliance
- Retention compliance

Decentralized approach

- User data remains anonymous
- User data cannot be passed to a third party



Prevent the possible abuse of data

Activity 2

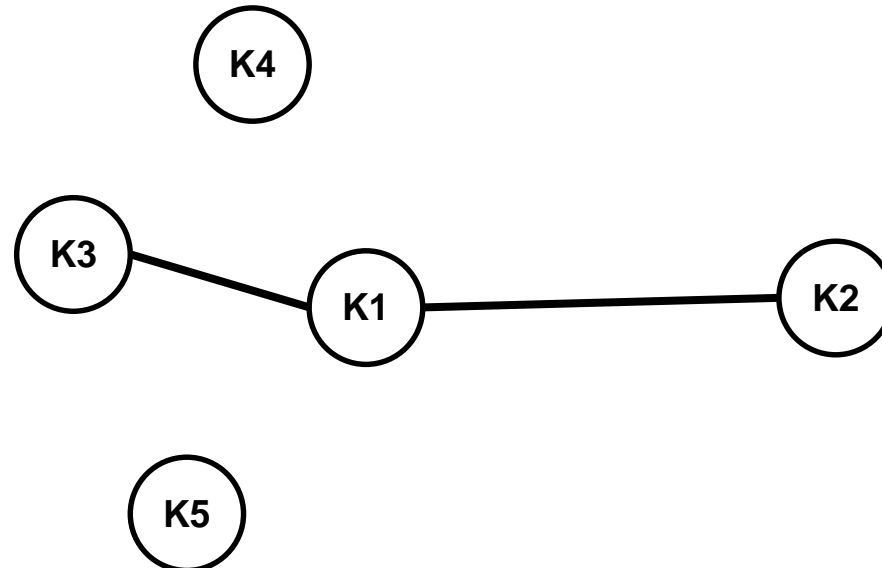
Data stored on device X (**key = K1**)

Key	Time
K3	t3
K4	t2
K2	t6
K5	t8

Data stored on device Y (**key = K2**)

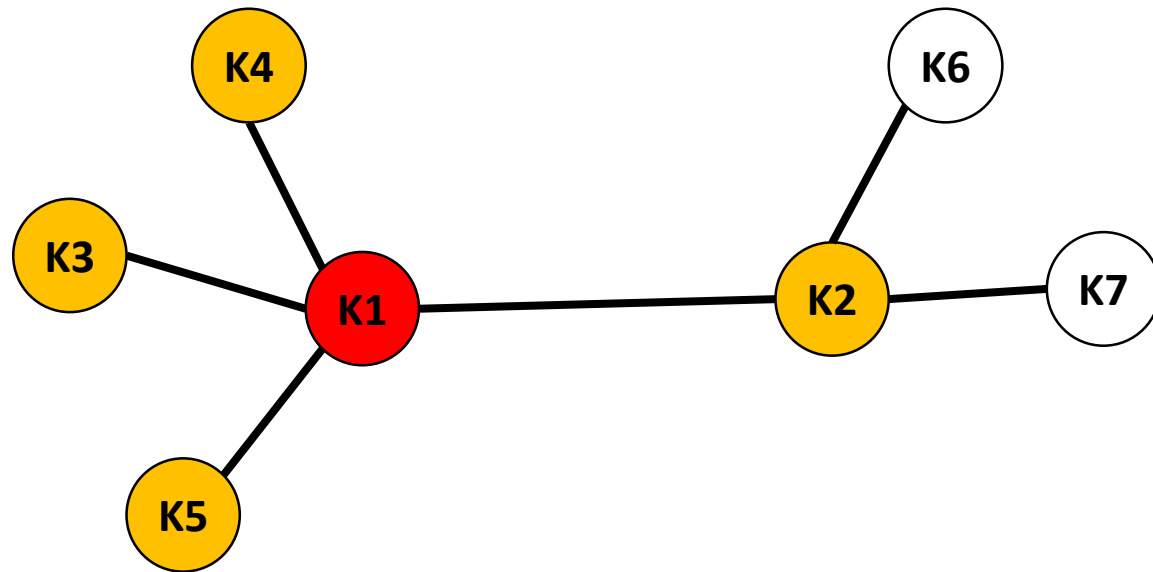
Key	Time
K1	t6
K6	t3
K7	t9

Recall that a contact tracing diagram is a graph where each node represents an individual and each edge represents a contact. You can use keys to show the nodes. Draw the contact tracing diagram for this data set.



Key	Time
K3	t3
K4	t2
K2	t6
K5	t8

Key	Time
K1	t6
K6	t3
K7	t9



- Additional information could not be extracted
- Could find people who should be notified

Gain

- Privacy protection
- Support for contact tracing

Loss

- Extensive research
- Identification of infected area
- Identification of gatherings that violate congregation or social distancing rules



Trade-off

Sahar: A public health official

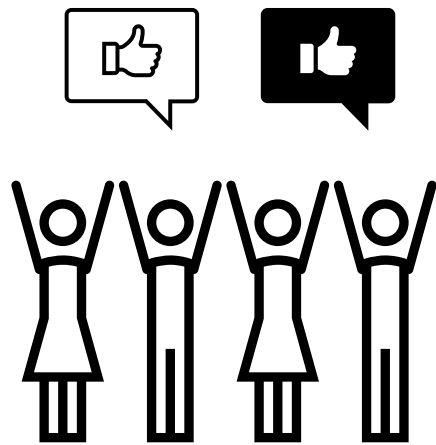
- Sahar is a public health official. Her main aim is to stop the spread of the virus. She wants an app that collects enough information to allow for effective contact tracing, but also protects the user's privacy enough that the app will be widely downloaded and used.



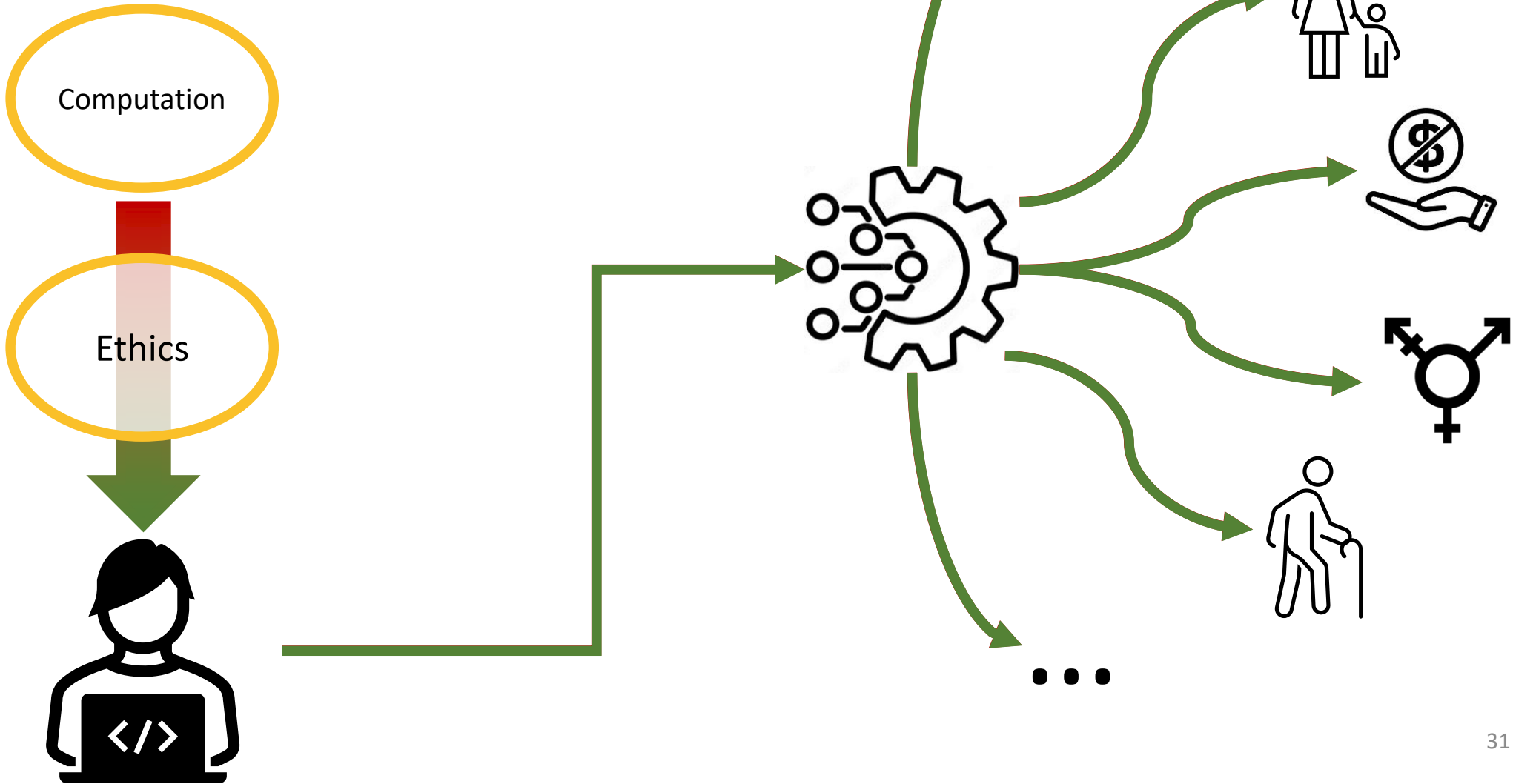
Inevitable trade-offs

- Sometimes we may be able to find a way to get both the privacy and public health we want
- But often, trade-offs will be inevitable--and different stakeholders will want different trade-offs





Ethics and computation





Activity

- With your team:
- Discuss ways that you can empower your project.
- Identify the user data that you need to fulfill the purpose of your product.
- Identify your stakeholders.
- Discuss any concerns or priorities that stakeholders might have about using your product.
- Discuss different designs and the trade-offs you have to make for each approach.