Embedded Ethics

The Ethics of Data Protection

Welcome to Embedded Ethics!

This embedded ethics module is a collaboration between philosophy and computer science.

The goal of embedded ethics is to tie ethics and computer science closely together, so you make ethical considerations in your work and research as computer scientists.

Today, we are going to help you understand:

- How file systems and permissions in UNIX work
- The differences between working on your own computer and a shared computer system
- The privacy concerns that come up when working on a shared computer system
- Some techniques for thinking about those privacy concerns

Part 1:

File Management in UNIX

What is a file?

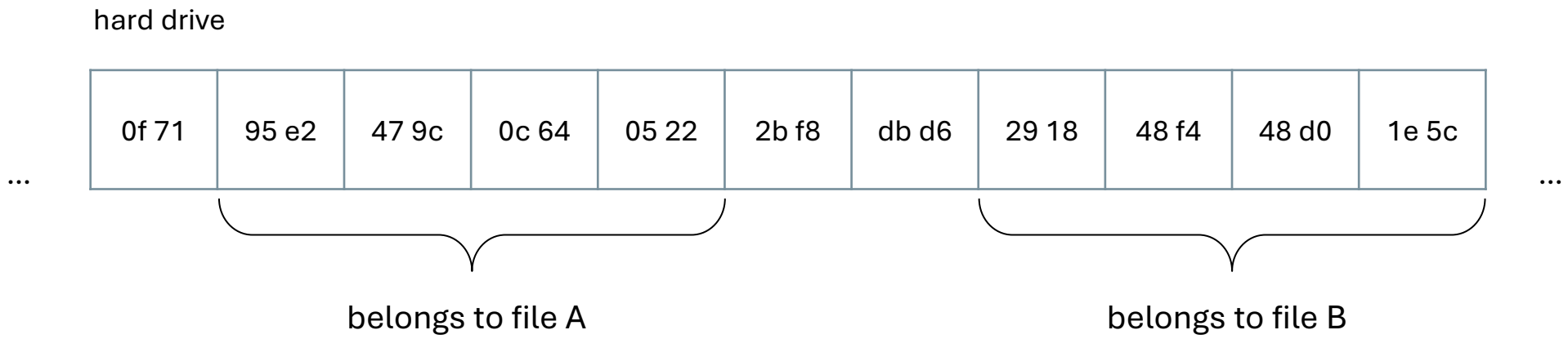
- Just a sequence of bytes stored “somewhere”.

What is a file system?

- More importantly, why do we need one?

Storage Media

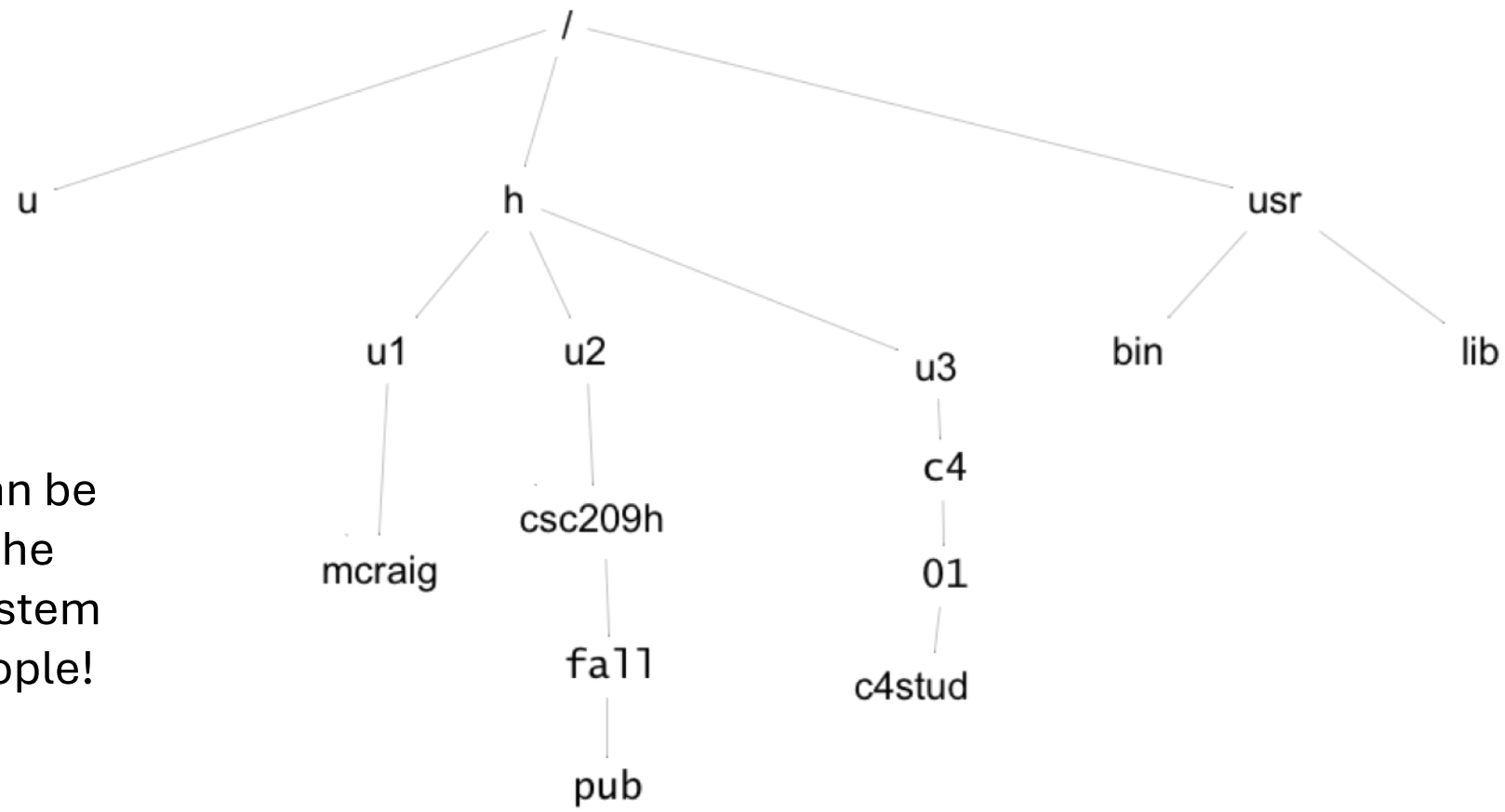
- E.g., hard drive, solid state drive, etc.
- Also just a (large) sequence of bytes
- File system is needed to organize files on a device



Unix/Linux File System

- Everything is a file!
  - Plain text documents are files.
  - Executables are files, e.g., gcc
  - Directories are also files!
- The “root” directory - named “/” - is the starting point
- A directory (folder) is a special file that contains mappings of filenames to their data and *metadata*
- Metadata is the information kept about a file
  - E.g., file size, file owner, permissions, last modified time, etc.

File System Directory Hierarchy



Your files can be stored in the same file system as other people!

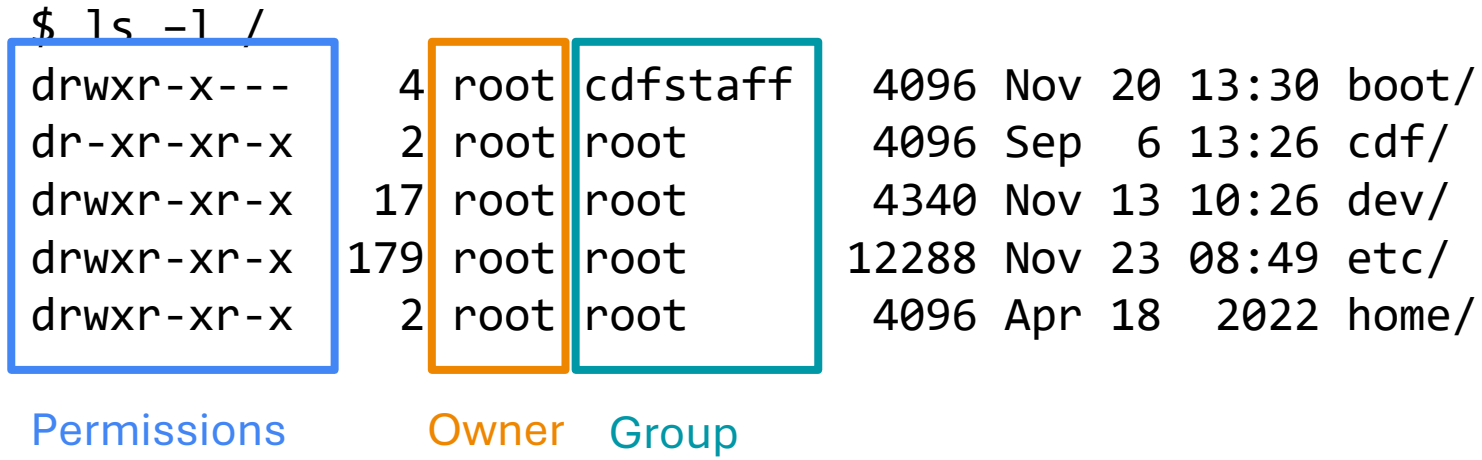
Shared Systems

- When you log into a lab workstation or remote log into teach.cs, you are using a shared system
- How does the file system know which files belong to you and prevent others from seeing or modifying them?

Permissions

- Every file and directory has an owner and a group
- Every file and directory has a set of permissions

- These mechanisms allow us to keep our own data private and also to share files with others



Permissions

Type of file
d = directory
- = regular file

	Read	**Write**	**Execute**
File	View contents	Modify contents	Load and run file
Directory	View directory contents (e.g. ls)	Add or delete files	“pass through”

Unix Group

- A set of users who can share files
- A user can belong many groups
  - You can be in the csc209 group, class of 2026 group, and utsg group.
- A file can only be set to one group
- The file owner does not have to be in the file’s group

Changing File Permissions

001	1	execute
010	2	write
100	4	read

- chmod 755 <filename>
  - 3 numbers between 0 and 7, the octal value for that category of user
  - Quiz — what is the command to set the permissions of the file classlist to be world readable but writeable only by the file owner and members of the group.
- Another approach
  - chmod u+rwx
  - chmod go-x
  - adds or removes permissions for those categories of users

Demo

When you shift from your own computer to a shared computer system, the biggest differences are:

Shared computational resources – raises questions about fairness

Shared file storage – raises questions about privacy

Part 2:

Privacy Harms

Consider each of the following items of information about you that might be stored on your server:

1) Chat history
2) Timetable
3) Grades
4) Last login time

Which item of information would you be most upset about having a hacker know about you?

Citron and Solove (2021)’s typology of privacy harms:

- Physical harms
- Economic harms
- Reputational harms
- Discrimination harms
- Relationship harms
- Psychological harms

Citron and Solove (2021)'s typology of privacy harms:

- Physical harms
- Economic harms
- Reputational harms
- Discrimination harms
- Relationship harms
- Psychological harms

Can you think of some ways that learning someone's last login time might cause them to suffer the highlighted harms?

Part 3:

Harmless Wrongs

Someone touches your cell phone while you are away. You never find out.

Was it wrong for them to touch your phone?

Imagine that someone goes into a folder on the shared system that you accidentally left public and views some of your information.

Suppose they do **nothing at all** with that information, and you never find out? Is it wrong of them to do so?

In these cases, someone is wronged, but they do not seem to be noticeably harmed. This is called a harmless wrong.

Can you think of other examples of harmless wrongs?

Harmless wrongs are puzzling! How can you wrong someone without noticeably harming them?

Some people think that harmless wrongs are impossible because of this argument:

1. You can only harm someone if they are aware of the harm.

2. You can only wrong someone if you cause them harm.

3. Therefore, you can only wrong someone if you cause them a harm that they are aware of.

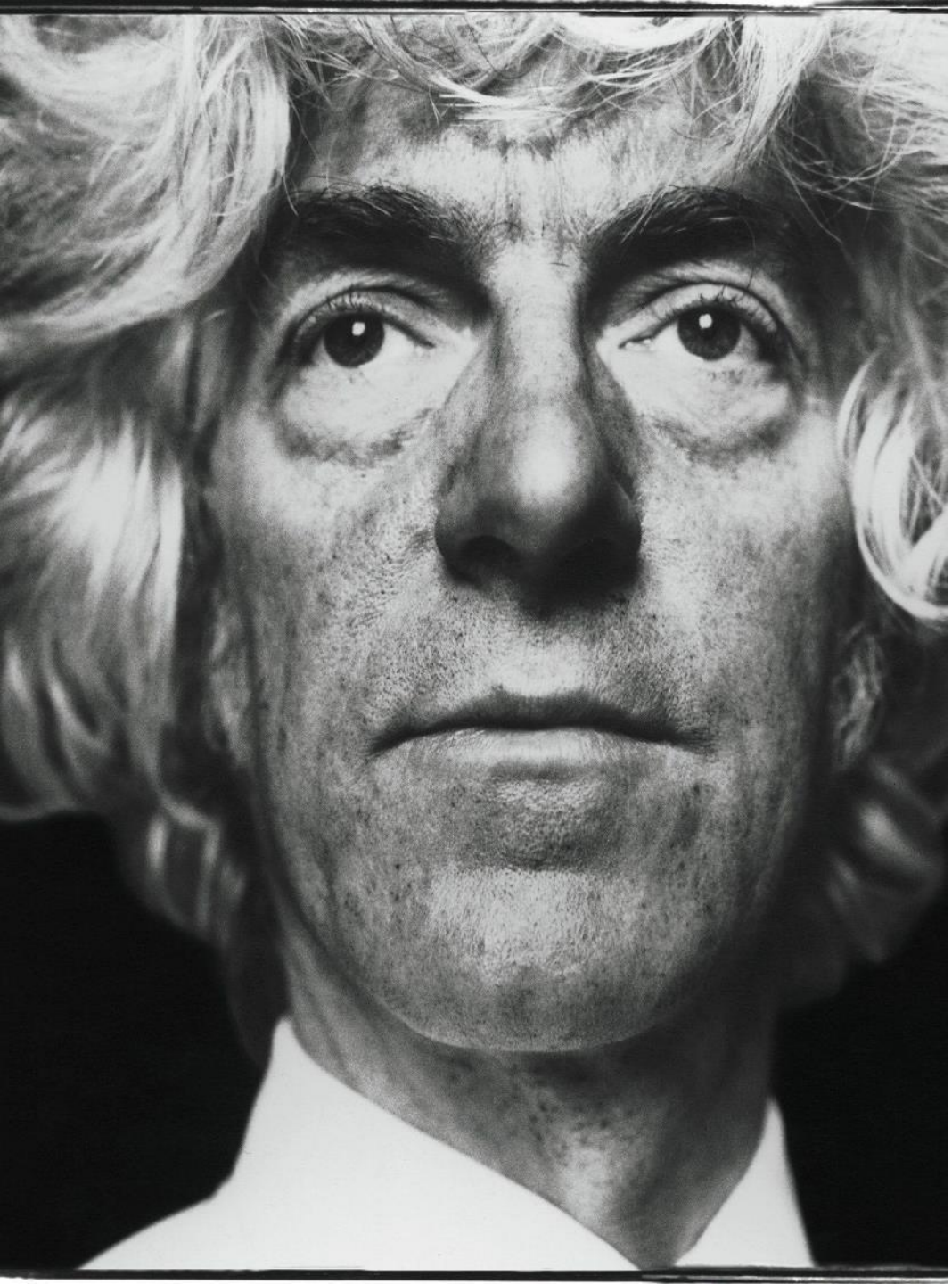
Some people think that harmless wrongs are impossible because of this argument:

1. You can only harm someone if they are aware of the harm.

Can you think of anything mistaken about this premise?

2. You can only wrong someone if you cause them harm.

3. Therefore, you can only wrong someone if you cause them a harm that they are aware of.

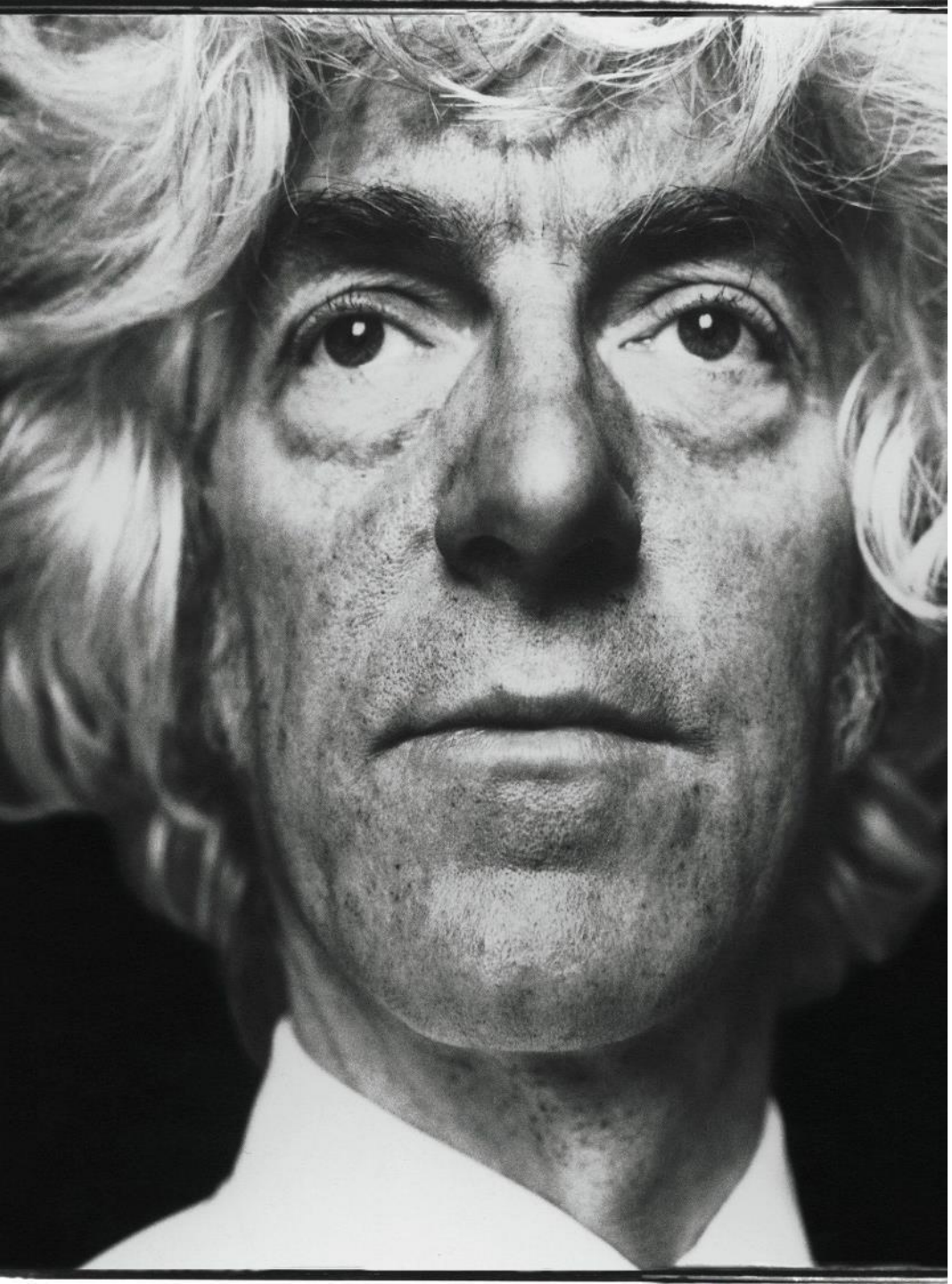


Philosopher Derek Parfit:

What things make our life *go well or go badly*?

Some are subjective (they depend only on what is *inside* your mind):

- Happiness, unhappiness
- Feeling like our desires are satisfied



Philosopher Derek Parfit:

What things make our life *go well or go badly*?

Others are objective (they also depend on things *outside* of your mind):

- Knowledge, ignorance
- Having our desires actually satisfied

Most people think that friendship is valuable – it makes your life go better.

Suppose that you have many friends, lots of good conversations with them, they affirm and support you....

… but actually, your friends don’t like you and they make fun of you behind your back, and you *never find out*.

Parfit: Your life has gone worse than if your friends really did like you!

Friendship itself, and not just the experience of friendship, is valuable.

Back to our argument:

1. You can only harm someone if they are aware of the harm.

2. You can only wrong someone if you cause them harm.

3. Therefore, you can only wrong someone if you cause them a harm that they are aware of.

Back to our premise:

1. You can only harm someone if they are aware of the harm.

Parfit:

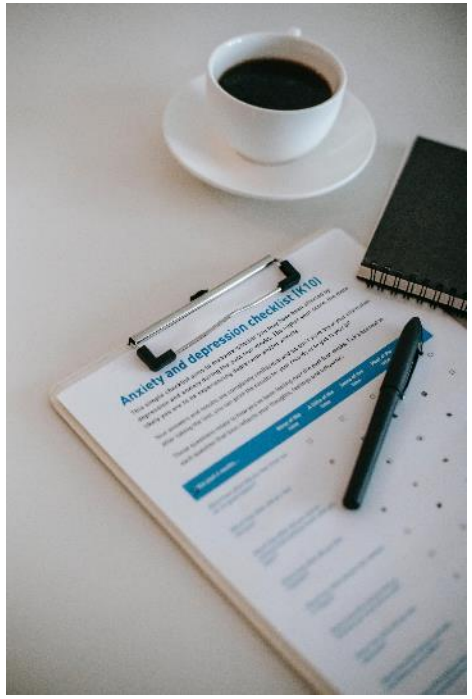
- Your life can be made worse by things that you are not aware of.
- So, you can be harmed by things that you are not aware of.
- So, the premise is incorrect!

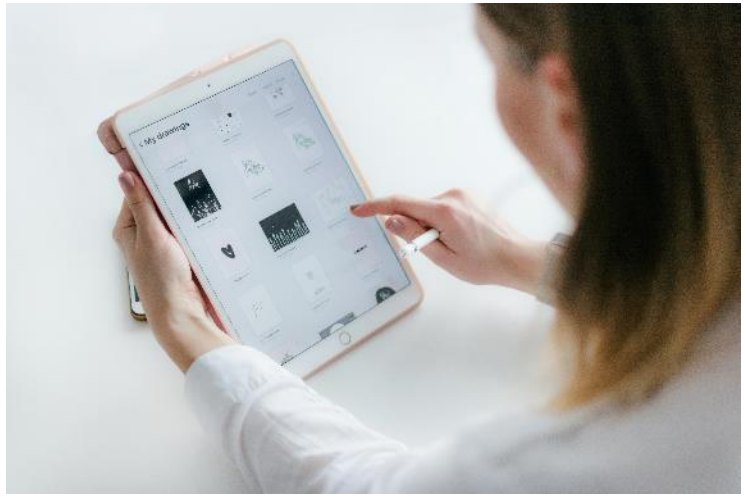
Why do harmless wrongs matter for computer scientists?

It’s tempting to think that it’s OK to snoop on people as long as you don’t do anything with the information…

But it seems like most of you have the intuition that there are harmless wrongs. You can wrong someone even if they are not noticeably harmed.

Why do harmless wrongs matter for computer scientists?





Many of you will be working with sensitive user data in your careers, internships and other positions!

Summary

Today we have explored:

- How file systems and permissions in UNIX work
- The differences between working on your own computer and a shared computer system
- How people might be harmed by losing their privacy
- How to describe an ethical problem using a premise-conclusion argument

Acknowledgements

This module was created as part of an Embedded Ethics Education Initiative (E3I) through the Department of Computer Science

Instructional Team:

Philosophy: Steve Coyne

Computer Science: Karen Reid, Jack Sun, Dee Kostas

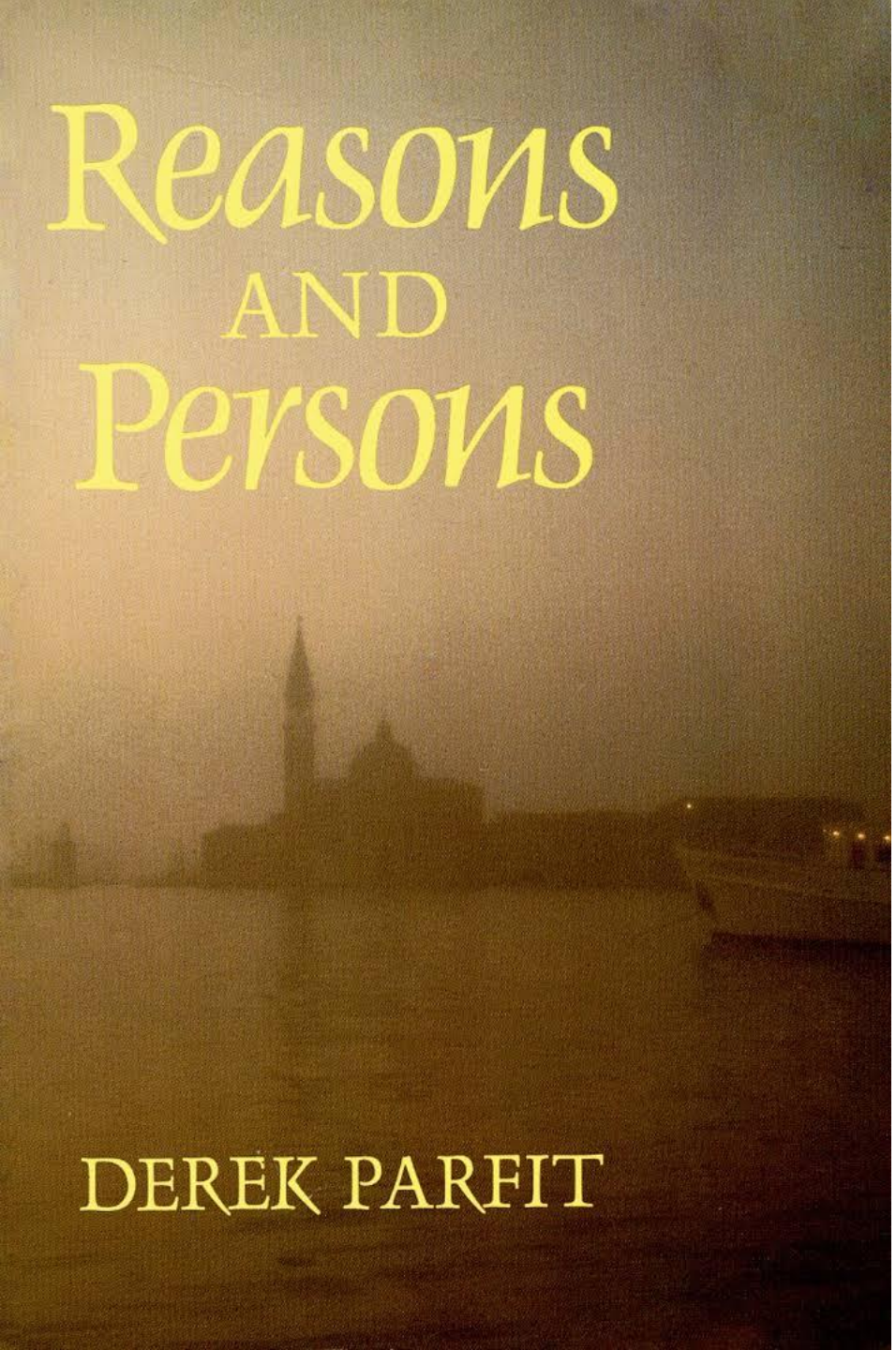
Faculty Advisors:

Diane Horton[1], David Liu[1], and Sheila McIlraith[1,2]

Department of Computer Science

Schwartz Reisman Institute for Technology and Society

University of Toronto



References

- Parfit, Derek. *Reasons and Persons*. (Oxford: Oxford University Press, 1984)
- Solove, Daniel J. and Keats Citron, Danielle, "Privacy Harms" (Washington: GW Law Faculty Publications & Other Works, 2021).