SIGPwny

FA2023 Week 10 • 2023-11-05

Ethics and Law

Anusha Ghosh

Announcements

- No meeting this Thursday!
  - ACM Bar Crawl is happening

ctf.sigpwny.com

sigpwny{i_am_NOT_a_lawyer}

Why should we care?

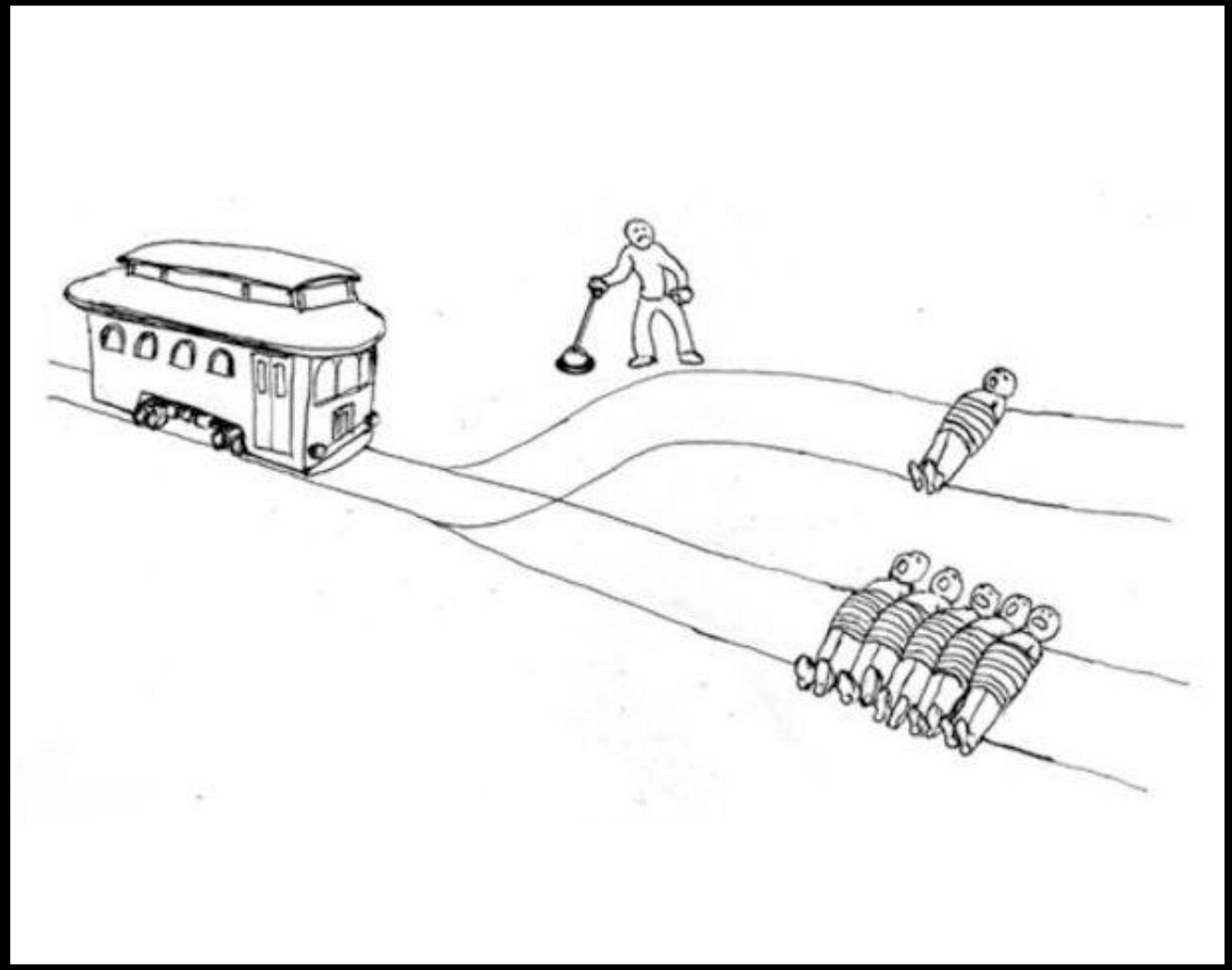
- Technology, especially computers, shapes our lives in important ways
- You hold a lot of power by learning the skills we teach
- You also have a lot of influence, even at bigger companies!

Moral Frameworks

Ethical Models

You are a switch operator near a trolley, the trolley is going down a track towards 5 people.

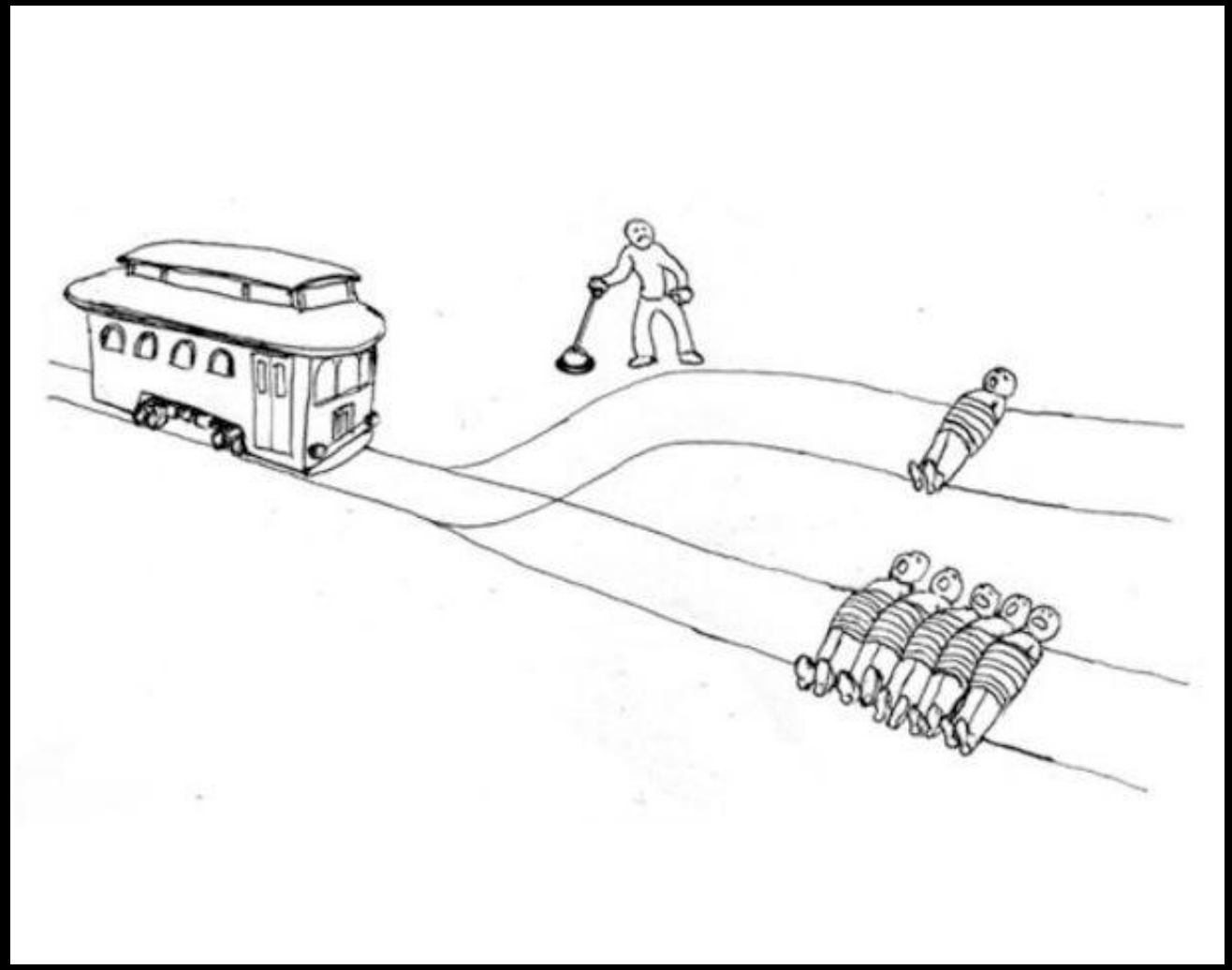
You can pull the switch and save the 5 people, but at the cost of one person.



Utilitarianism (Consequence-Based)

Whatever causes the most social good or "utility" is the action that should be taken. The **outcome** is ultimately what matters.

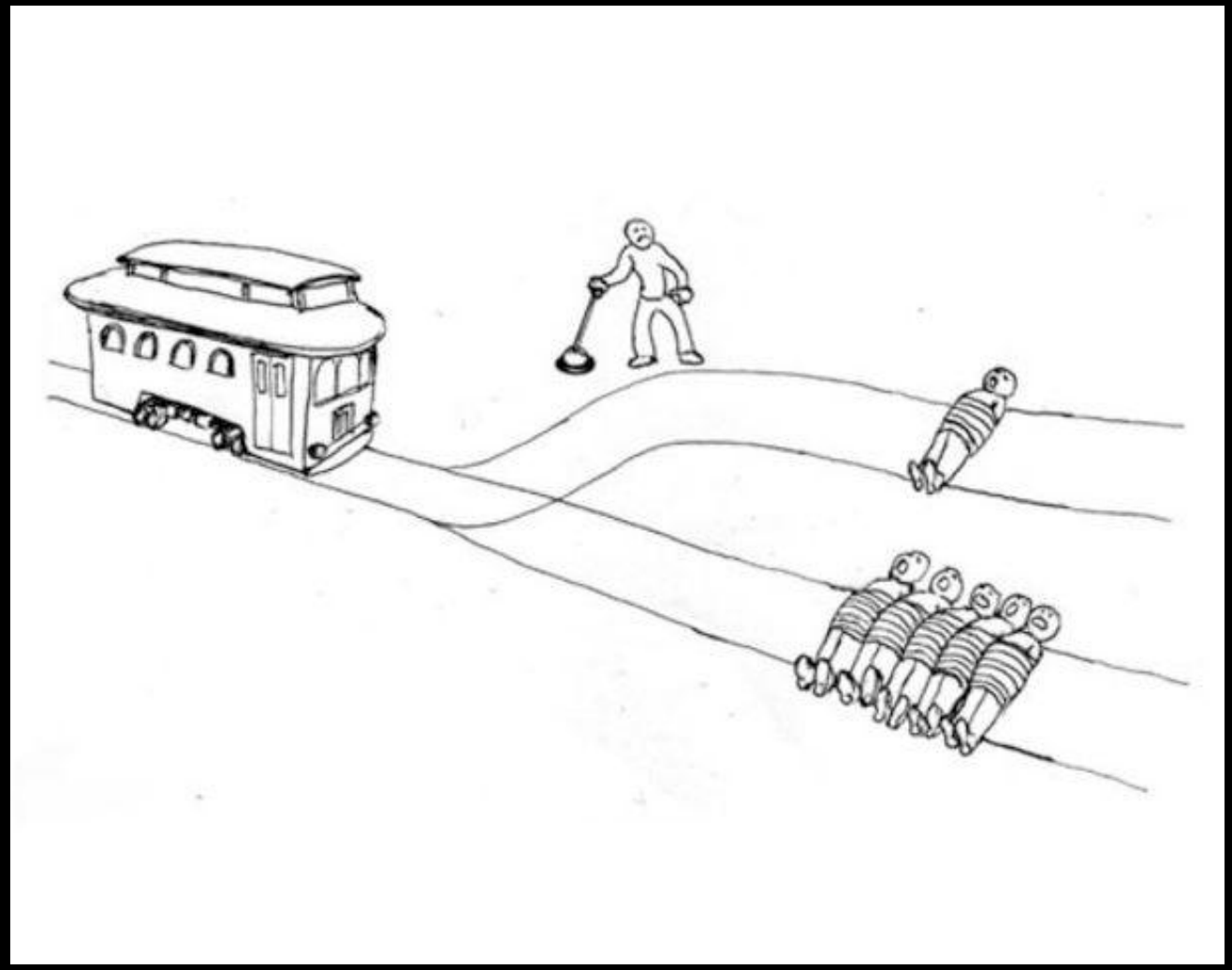
How would a **utilitarian** navigate this ethical scenario?



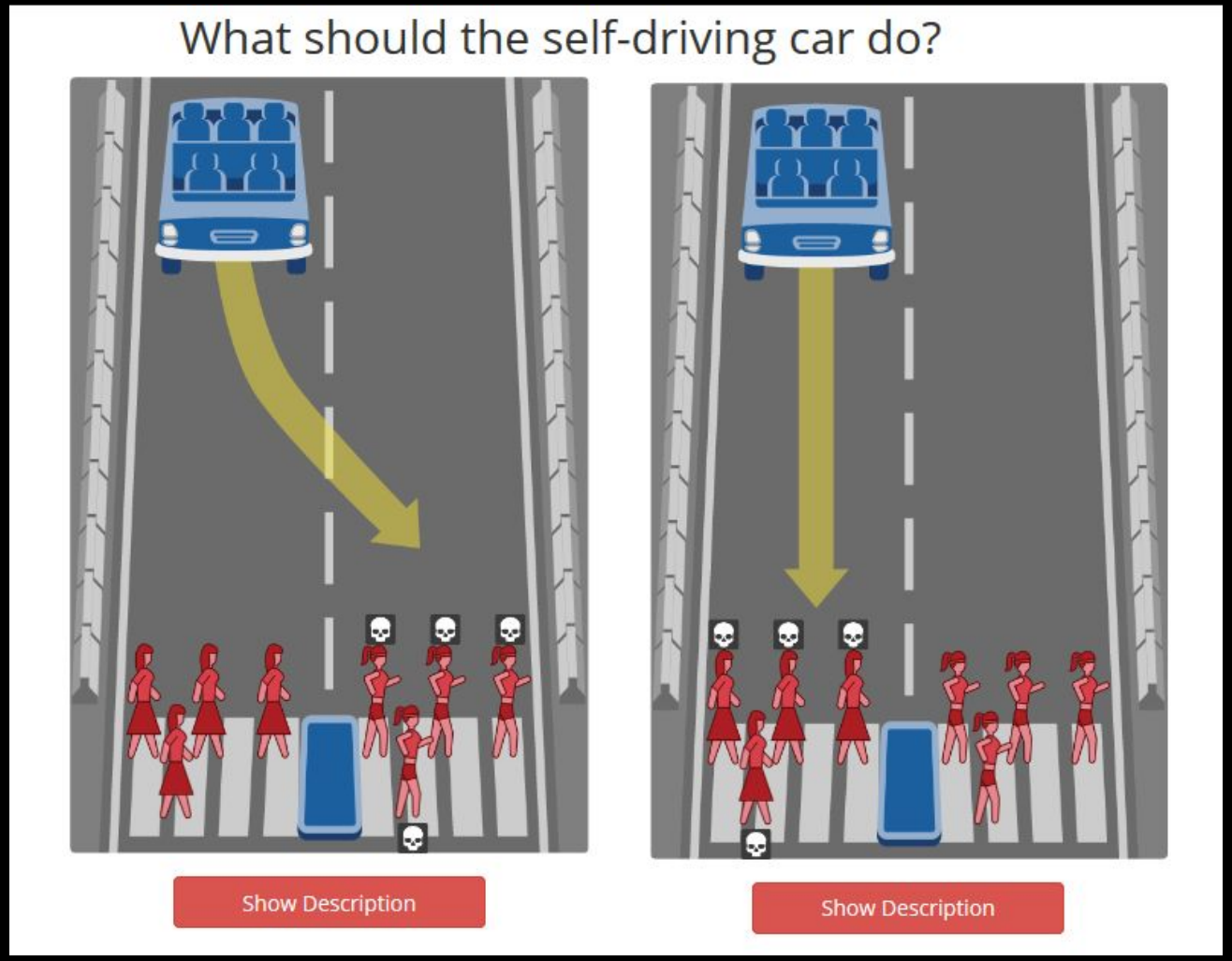
Deontology (Duty-Based)

1. All **moral agents** have a duty to uphold a universal set of rules to each other.
2. Intent is what really matters in an action's morality, regardless of outcome.
3. Moral agents should not use other moral agents as a means to an end.

What would a **deontologist** do in this situation?



What should the car do?



Hacker "Hats"

White Hat
Hacks for the purpose of protecting others

Black Hat
Using cybersecurity for malicious intent: going sicko mode.

Grey Hat
A little bit of good, a little bit of bad. Maybe a little sus

Security Ethics

- Mitigating Risk
  - Risk = Expectation of loss expressed as probability
- Hacker "Ethics" (Stephen Levy)
  1. Access to computers should be unlimited.
  2. All information should be free.
  3. Mistrust authority.
  4. Hackers should be judged by their skill.
  5. You can create art and beauty on a computer.
  6. Computers can change your life for the better.

Ethical Security Research

- Hack systems with
  - Explicit Permission
  - Expertise
  - Proper documentation
- Not having all three can put you in massive trouble

Ethical Vulnerability Reporting

Vulnerability Disclosure

- Nondisclosure
  - Keep it secret, sell it secretly, use it for your own gain.
- Full Disclosure
  - Tell everyone, just drop it.
  - Make sure people can protect themselves from the vulnerability.
- Limited Disclosure
  - Privately disclose to the vendor only so they can develop a patch.
  - Risky because you can be attacked legally for this.

Responsible Disclosure

- Disclose vulnerability in private to the company
  - Do this ONLY IF THEY ARE NOT A SHITTY COMPANY
- Talk to vendor and agree on deadline for full disclosure
  - For example, Google's deadline is typically 90 days
- Maintain communication with both parties during patch dev
- Fully disclose vulnerability when patched / after deadline

Other Ethical Issues

Incident Response

When should information about an attack be shared? Should intruders be kicked out first or should systems get back up? What information should be shared?

Attribution

Can we really be sure that it was <PERSON> who committed the attack?
Information is easily falsifiable.

Hack-Back

If an organization is under attack (company), is it ethical for them to respond in kind?
"Active Cyber Defense Certainty Act" amends CFAA and allows for hack-back with "high degree of certainty"... what about that falsification thing?

The Law

please don't go to jail

What Makes a Crime

- Elements that make up a crime
  - Specified **state of mind** or **intent**
  - Performance of a prohibited act
- Intent
  - Mens Rea = "requisite guilty state of mind"
  - Intent Definitions Under the Law
    - Purposefully: you hoped for that outcome to happen, you tried to make it happen
    - Knowingly: you knew the outcome was certain/probable even if it was unwanted
    - Recklessly: you consciously ignored known risks
    - Negligently: you should have been aware of the risks, but you were not

CFAA Intro

18 U.S. Code § 1030 - Computer Fraud and Abuse Act

- Enacted 1986
  - Hasn’t been updated much since then
- Very arbitrary and unclear
  - Written by people who didn’t know much about computers
- Protects computers used by either a financial institution, the government, or used for interstate commerce
  - This has now come to define basically any computer

Sections of the CFAA

1. Obtaining classified information to injure US or aid foreign power
2. Accessing a computer without authorization **or exceeding authorized access** and obtaining information
3. Unauthorized access to US govt computers
4. Another federal crime combined with unauthorized access
5. Unauthorized access + damages
6. Computer password trafficking
7. Extortion + any of 1-6

Notable CFAA exceptions

- Data-in-transit laws (MITM != CFAA?)
- Wire fraud
- Mail fraud

Problems with the law

- Very outdated
- Doesn’t cover ethical hacking
  - Supreme court won't make decisions (Van Buren v. US)
- Arbitrary (what defines reasonable access etc.)

Next Meetings

`2023-11-09` • **This Thursday**

- No meeting!
- Enjoy ACM Bar Crawl!

`2023-11-12` • **Next Sunday**

- TBD :)

ctf.sigpwny.com

`sigpwny{i_am_NOT_a_lawyer}`

Meeting content can be found at sigpwny.com/meetings.

SIGPwny