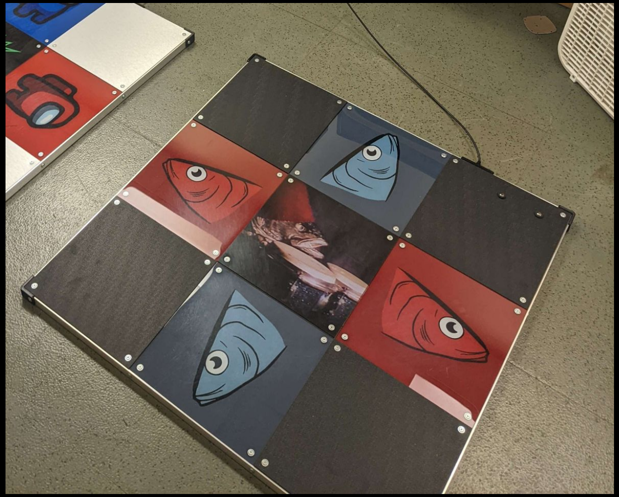
FA2022 Week 06

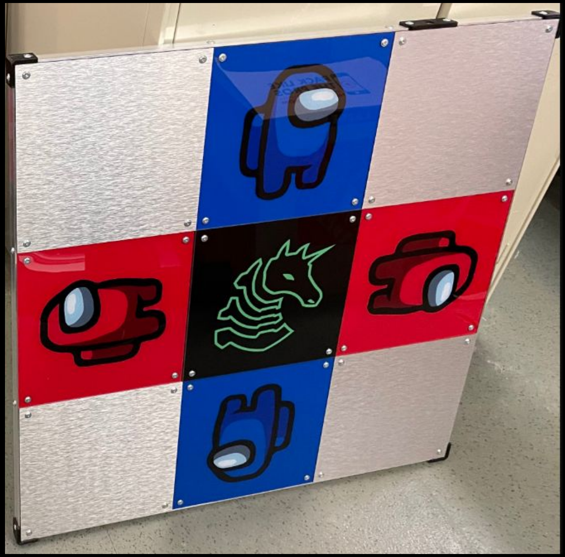
Ethics and Law

Thomas Quig

Announcements

- ACM Clean up party
  - Dates:
    - Saturday 2022-10-09 3:00PM
    - Saturday 2022-10-16 3:00PM
  - We get a dedicated DDR area!





ctf.sigpwny.com

sigpwny{i_am_NOT_a_lawyer}

ANOTHER ISP'S FILTERING CONTENT.
THANK GOD FOR CRYPTO.
IT WASN'T THAT LONG AGO THAT RSA WAS ILLEGAL TO EXPORT. CLASSIFIED A MUNITION.
YOU KNOW, I THINK THE CRYPTO COMMUNITY TOOK THE WRONG SIDE IN THAT FIGHT. WE SHOULD'VE LOBBIED TO KEEP IT COUNTED AS WEAPONRY.
WHY?
ONCE THEY GET COMPLACENT, WE BREAK OUT THE SECOND AMENDMENT
...DAMN.

Ethics (What not to do)

Tech people can be assholes sometimes

Examples of what not to do

Theranos - Ponzi Scheme

Facebook - Cambridge Analytica

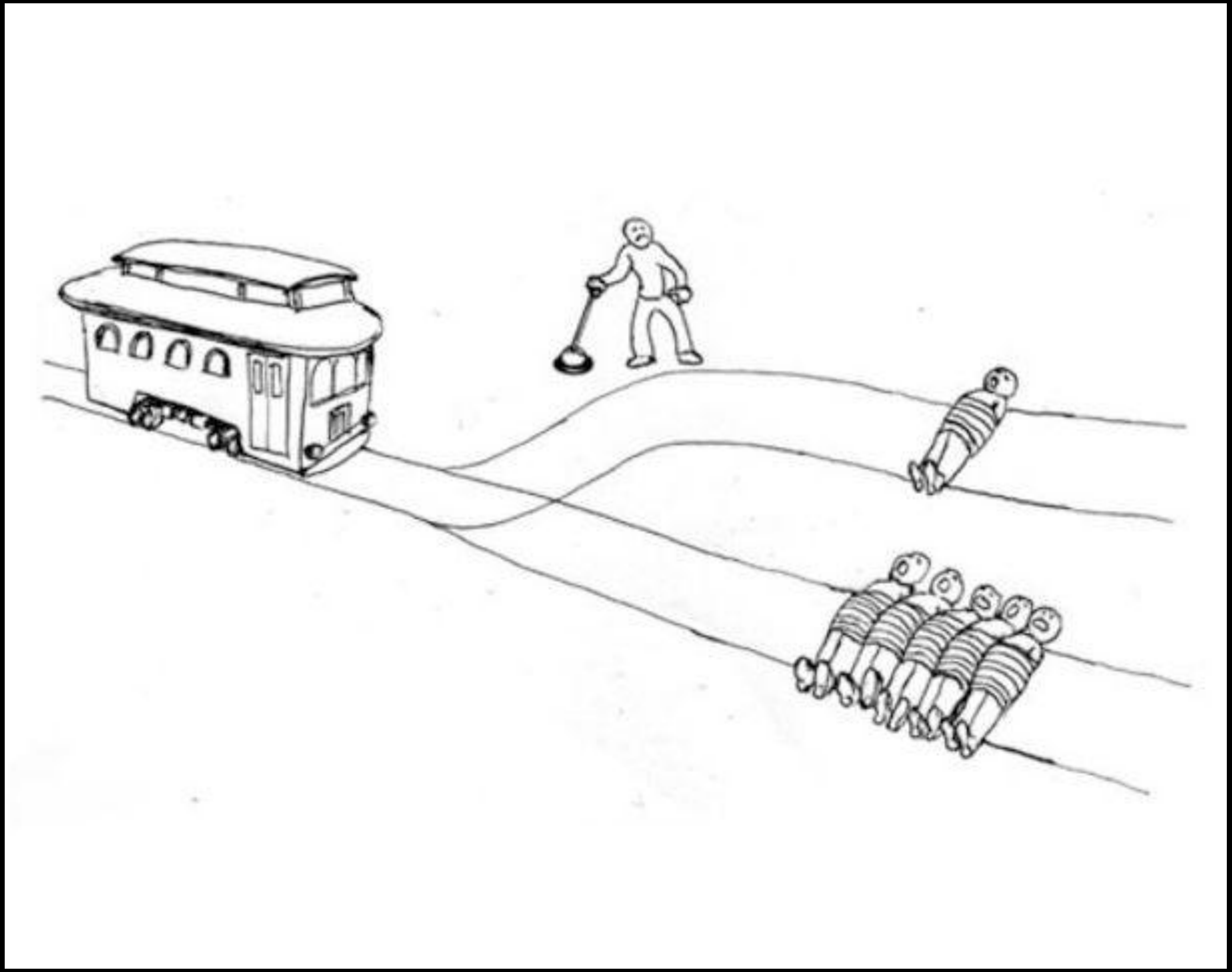
The NSA - Spying on every single citizen

Moral Frameworks

Ethical Models

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

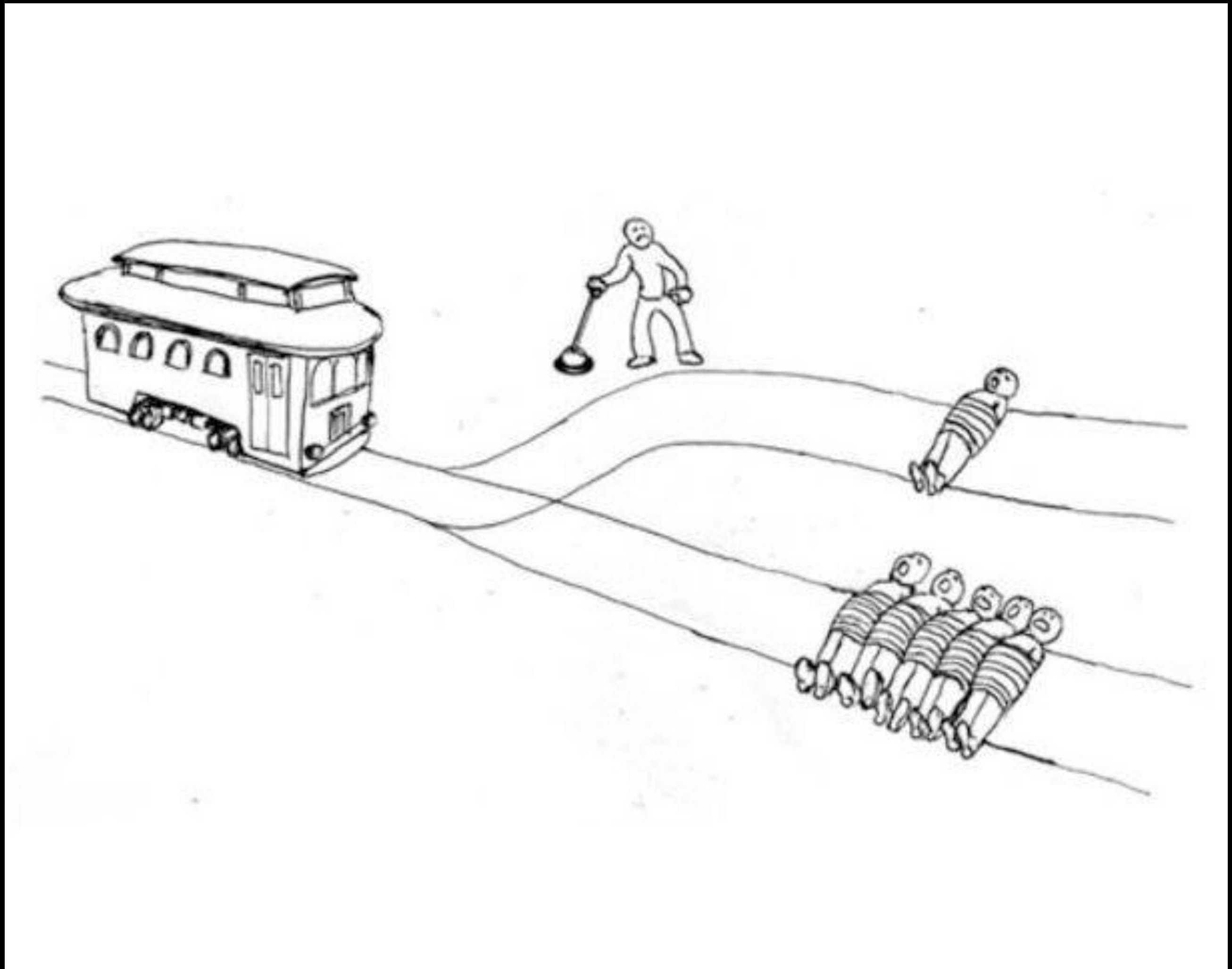
You can pull the switch and save the 5 people, but at the cost of one person.



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?



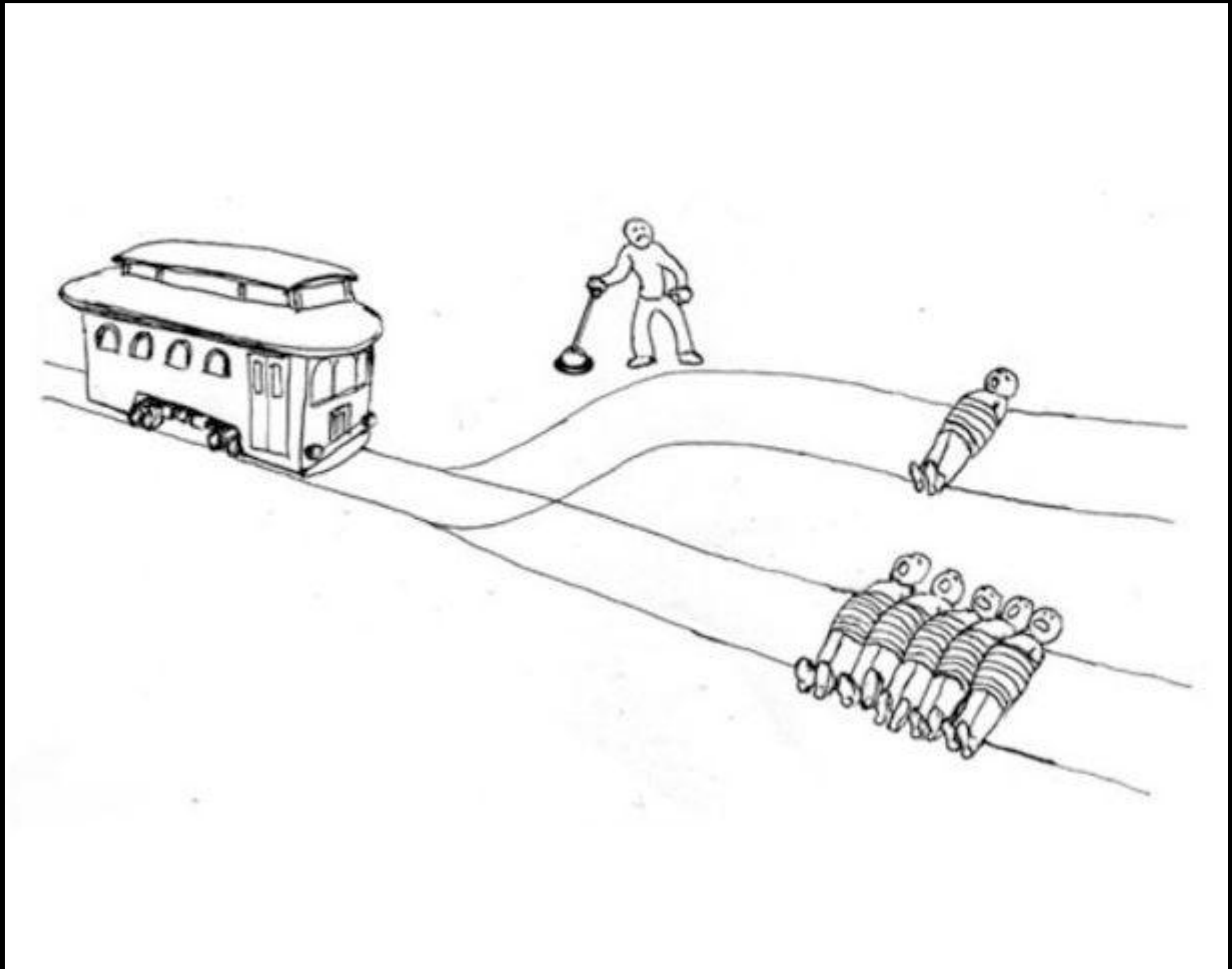
Deontology (Duty-Based)

Kant came up with this one, the "Categorical Imperative"

3 Parts

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?

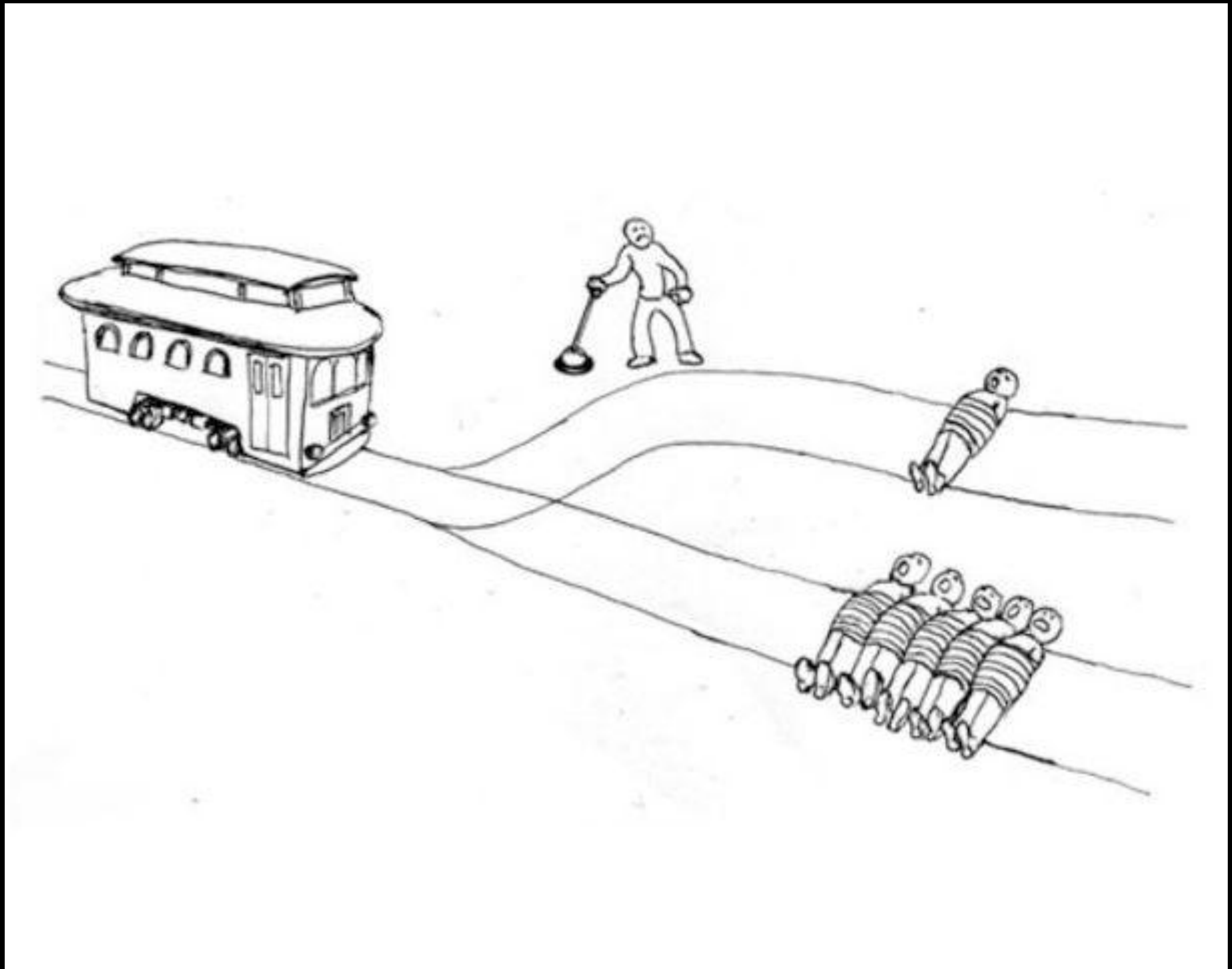


Virtue Ethics (Character Based)

Moral Agents should appeal to a set of good morals. The composition of one's character is what defines morality.

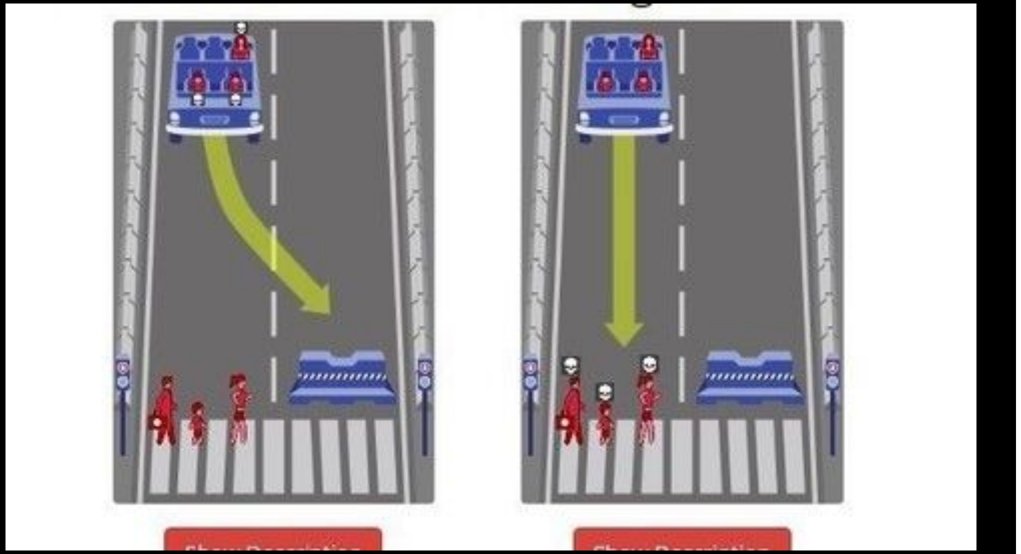
Actions are ethical if they adhere to good virtues. "Honesty, dignity"

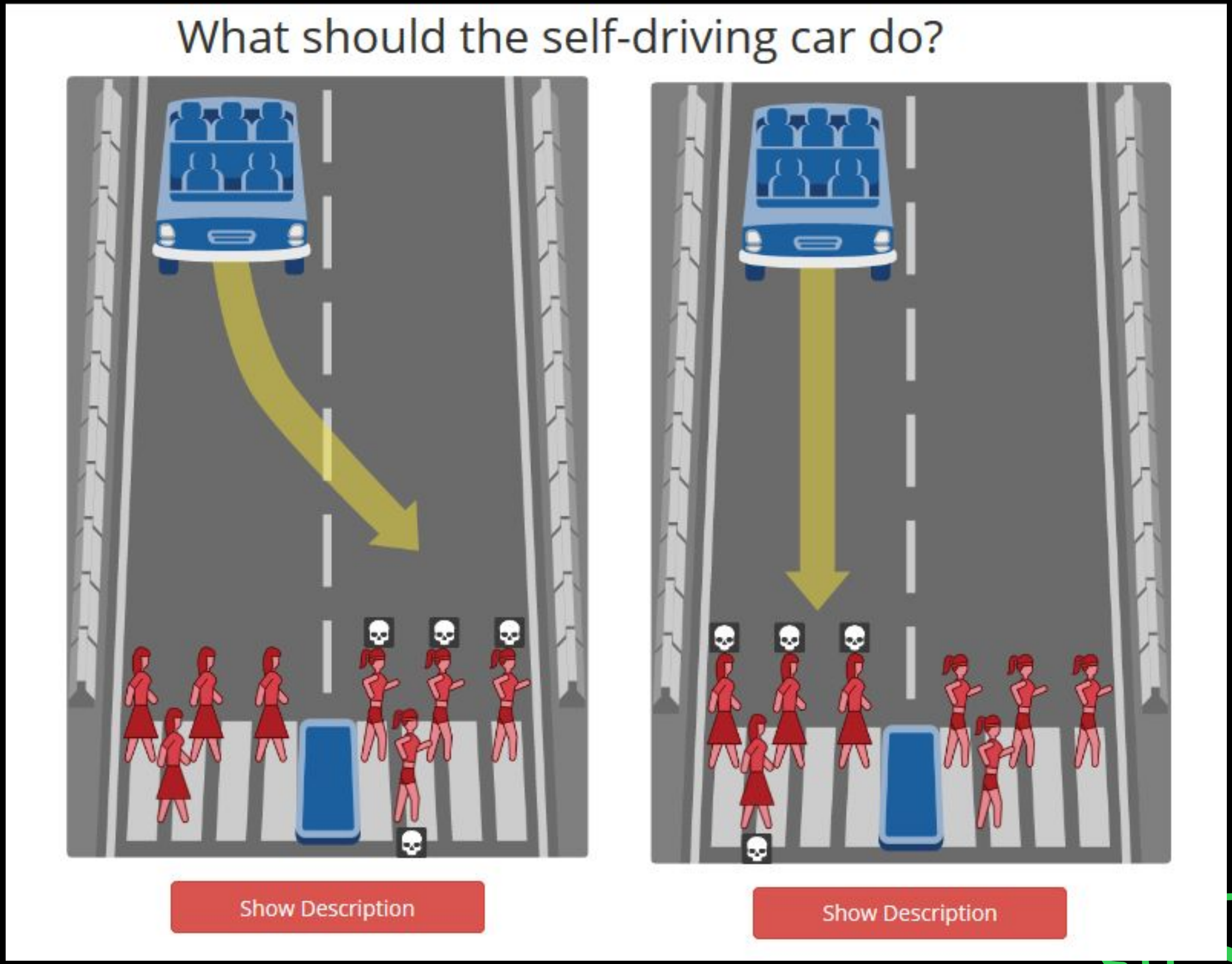
How would someone adhere to virtue ethics in this situation?



Relevance

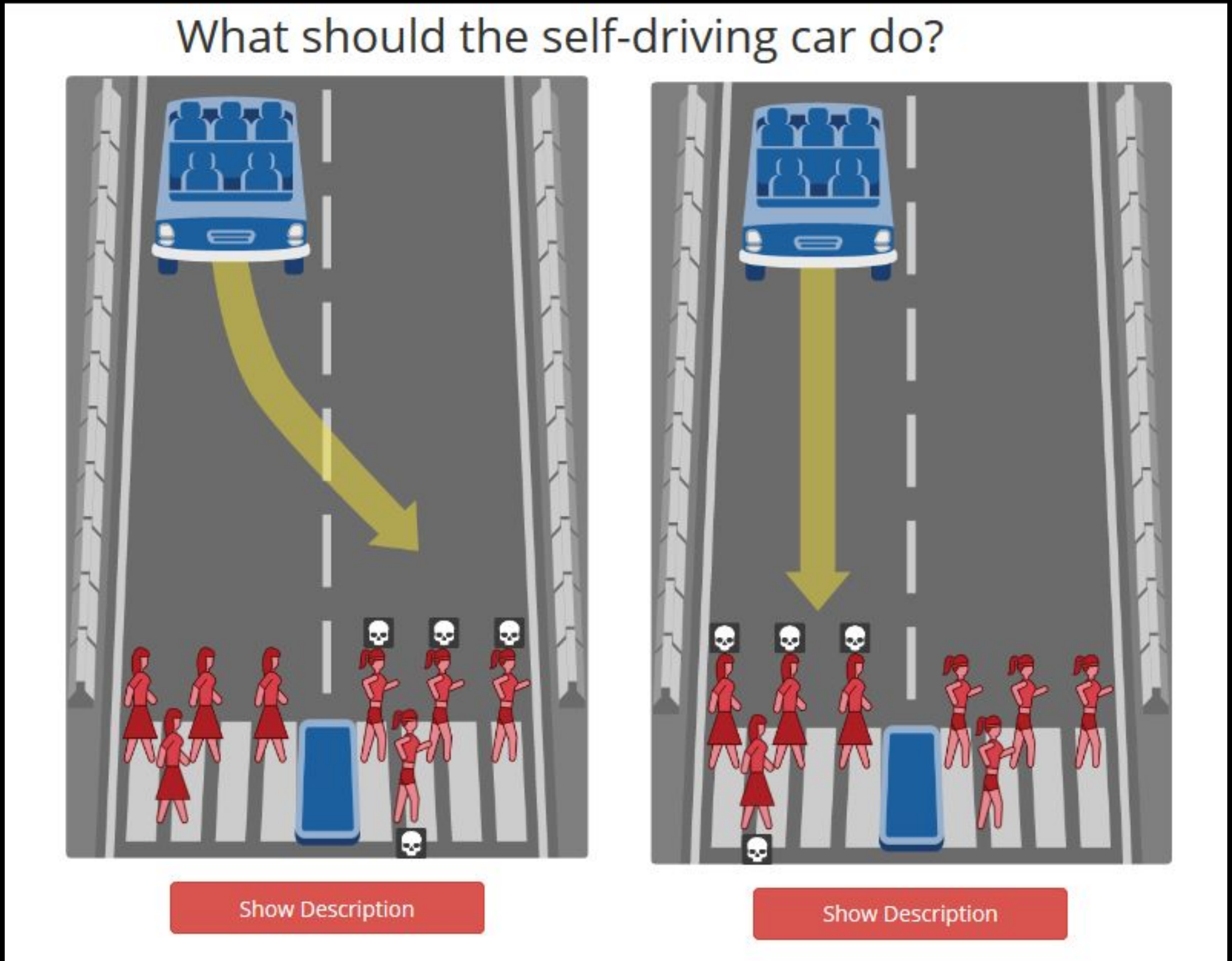
This applies in tech!





What should the self-driving car do?

What does the car do?



What should the self-driving car do?

How this applies to security?

Incident Response

Vulnerability Research and Reporting

SocEng attacks etc.

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.

Problems with Levy's Ethics

If information is free, write your Credit Card # on the board

Activities in cyberspace are virtual

- Separation of virtual and real

Hacker "Hats"

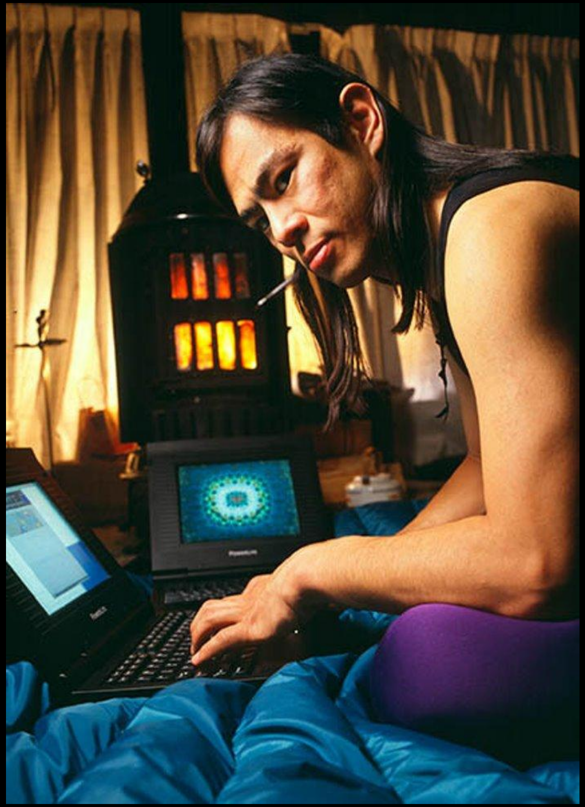
White Hat
Hacks for the purpose of protecting others

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

Ethical Security Research

- Hack systems with…
  - Explicit Permission
  - Expertise
  - Proper documentation



Ethical Vulnerability Reporting

Vulnerability Disclosure

- Nondisclosure
  - Keep it secret, sell it secretly, use it for your own gain.
- Full Disclosure
  - Tell literally everyone, just drop it.
  - Make sure people can protect themselves from the vuln.
- 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

1. Disclose vulnerability in private to the company
   a. Do this ONLY IF THEY ARE NOT A SHITTY COMPANY (More info later)
2. Talk to vendor and agree on deadline for full disclosure
   a. Google’s is 90 days
3. Maintain communication with both parties during patch dev
4. Fully disclose vulnerability when patched / after deadline

Bug Bounties

Hackerone!

Pwn2own

Company Specific Bug Bounty

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 really 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

Crimes

There are lots of them

Misdemeanor vs Felony vs Capital

State vs Federal

Civil court!!!

I have a love-hate relationship with these images

What Makes it a Crime

Two Elements that make up a crime

1. Specified **state of mind** or **intent**
2. Performance of a prohibited act

Intent

- Mens Rea = "Requisite Guilty State of Mind"
    - Intent to do crimes
- Specific vs General Intent vs Criminal Negligence
- 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, you didn't intend / want it, but you knew it would happen
    - Recklessly: You consciously ignored unjustifiable risks that you knew were risks
    - Negligently: You should have been aware of the risks, but you were not

Crimes (But like not really, but also yes... but like kind of...)

Solicitation - Asking

Facilitation - Assisting

Conspiracy - Planning

Attempt - Trying

Notes on Conspiracy

1. Agreement by two or more people to commit a specific crime
2. Must be COUPLED WITH OVERT ACT toward commission of crime
    a. Overt act != Illegal

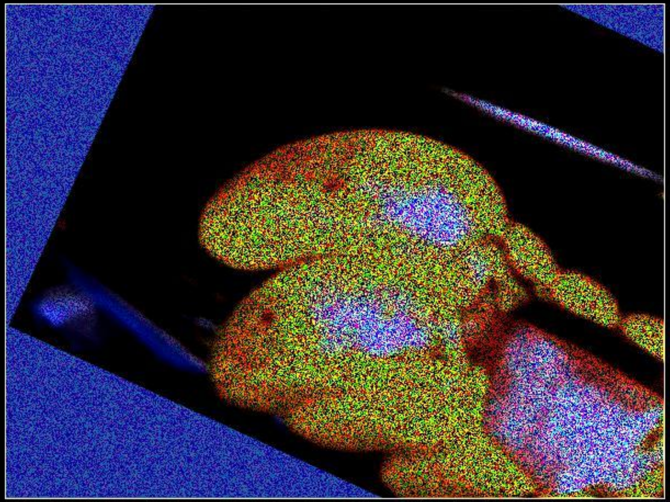
Types of Crime: Blue

Theft

Assault v. Battery

Mayhem

Murder (1st Degree, 2nd Degree, 3rd Degree)



Drug Abuse Violations

Types of Crime: White

Tax Evasion

Financial Crimes

Fraudulent Businesses (Pyramid/Ponzi Schemes)

Money Laundering

Mailing Threatening Communications

Types of Crime… Neither?

Fraud

CFAA Violations

Harassment

Etc.

This is not about what is right

This is about what exists

The Law (CFAA Part One)

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

- Enacted 1986
  - Hasn’t been updated much since then
- Protects Data At Rest
- Very arbitrary and unclear

We could spend a whole semester talking about this, so I will try to give a super brief summary of the whole thing.

The Law (CFAA Part Two)

7 Distinct Crimes

1. Obtaining classified information to injure US or aid foreign power
2. Accessing a computer without auth
   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

The Law (Not the CFAA)

- Data-in-transit laws (MITM != CFAA?)
- Wire fraud
- Mail fraud
- A thousand other pieces of law
    - Never ever ever ever ever find yourself violating CSA laws

Problems with the Law

Very outdated (made for 70s and 80s!)

Doesn’t cover ethical hacking. Supreme court won't make decisions (Van Buren v. US)

Arbitrary (what defines reasonable access etc.)

Tips (from not a lawyer!)

When in doubt, ask for permission before you do **anything**

Check what the company is, No criminal != you won't get sued.

Be quiet, get a lawyer, "anything you say can be used against you"

Be educated, know your rights, know the law

Next Meetings

2022-10-13 **- This Thursday**

- Crypto I
- Cryptography fundamentals - basic XOR and RSA encryption

2022-10-16 **- Next Sunday**

- Crypto II
- Advanced cryptography - hard RSA encryption and Diffie-Hellman key exchange

SIGPwny