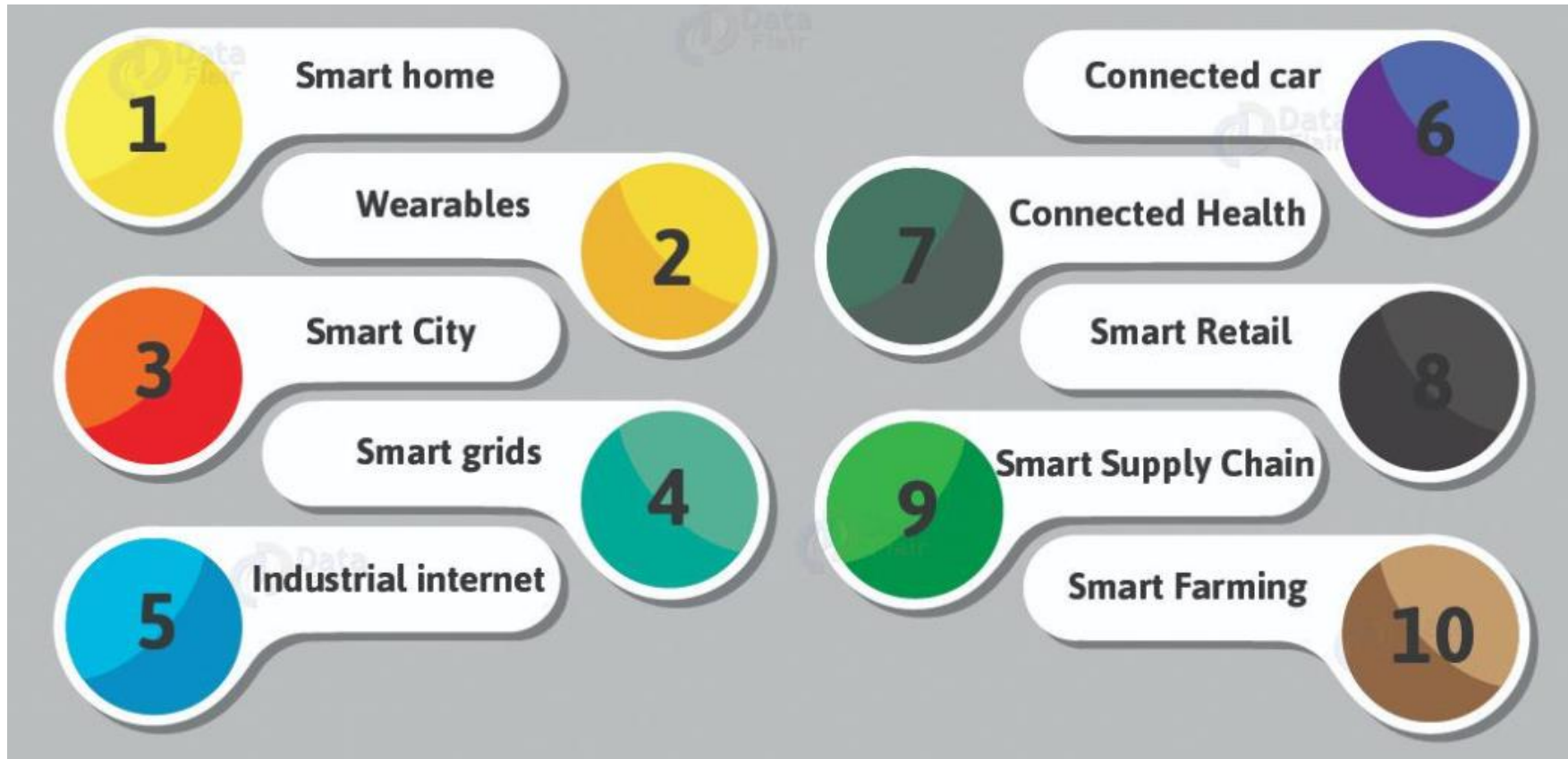




<https://futureoflife.org/ai-principles/>

(Human) Values In Computing

Smart Networked Technology



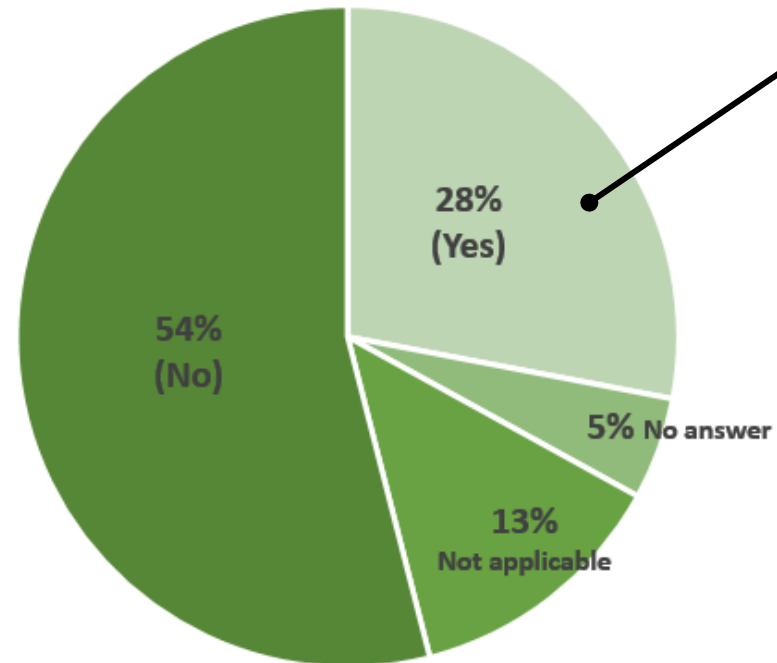
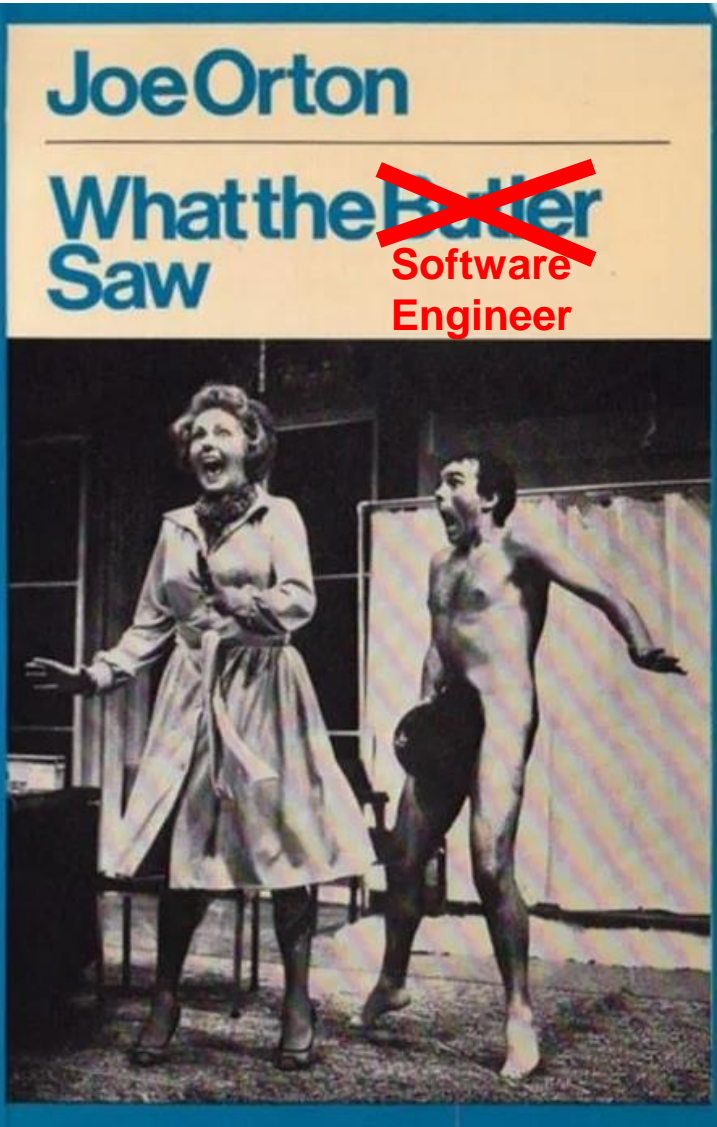
My story (Lucy)

- Coding on BBC Micro, ZX81, ZX Spectrum (1980s)
- MEng Engineering Science + MSc Information Systems
- Software Engineer & IT Consultant (UK wide, 10 years)
- IT Volunteer with VSO (Kathmandu, Nepal, 2 years)
- IT Business Analyst (Freelance, 10+ years)
- The National Museum of Computing (Bletchley Park)
- MSc Cyber Security (Insider Threats)
- PhD Computer Science (Whistleblowing)
- Teaching (Professional Ethics, Software Design, Group Projects)
- Business Analyst, ISS at Lancaster University



Do IT Professionals see harmful situations?

Have you experienced a situation at work where *decisions* were made about the design, creation or marketing of technology that you felt could have negative consequences for people or society?



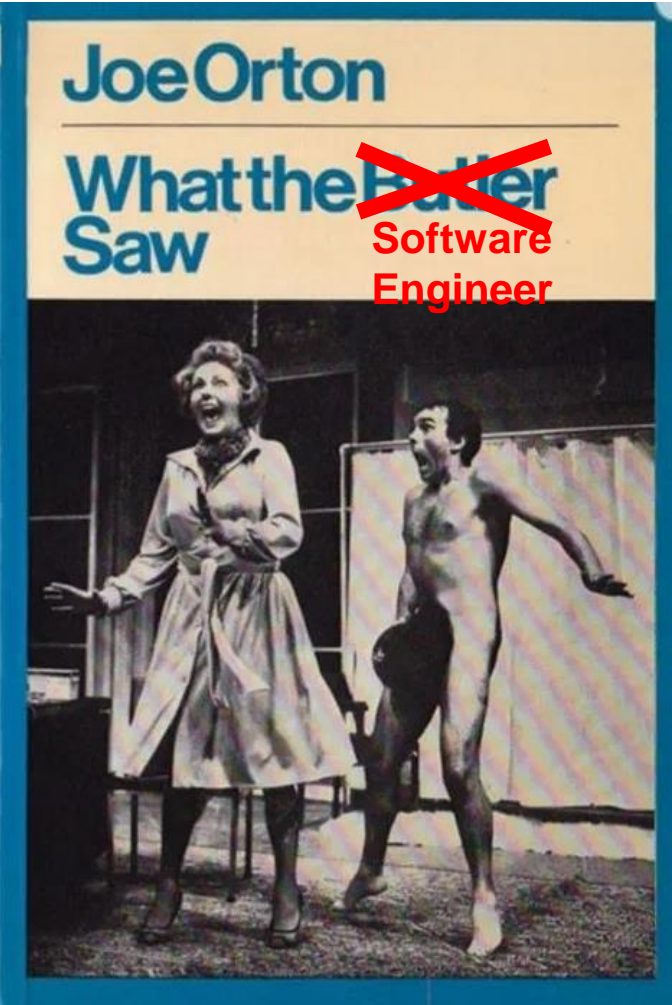
Harm:

- safety and security failures
- testing practice failures
- end user isolation or addiction
- job losses due to automation
- putting profit before people
- lack of knowledge and training
- lack of choice and control
- reliance on machines
- immoral practices
- misuse and abuse

Miller and Coldicott. People, Power and Technology: The tech workers' view (Ipsos MORI surveyed 1010 technology professionals, 2019)
385,000 programmers and software development professionals in the UK (UK Office for National Statistics, 2019)

What actions do IT Professionals take?

[of the 287 people that indicated they had seen potentially harmful situations]



90%
took
some action



Miller and Coldicott. People, Power and Technology: The tech workers' view (Ipsos MORI surveyed 1010 technology professionals, 2019)

Issues serious enough to leave or report outside of company

DuckDuckGO: “tracking is *creepy*”

The search engine & the value of privacy

www.wired.com/2011/01/duckduckgo-google-privacy/



Google Project Maven Walk Out (2018)



<https://static01.nyt.com/files/2018/technology/googleletter.pdf>

Dear Sundar,

We believe that Google should not be in the business of war. Therefore we ask that Project Maven be cancelled, and that Google draft, publicize and enforce a clear policy stating that neither Google nor its contractors will ever build warfare technology.

Google is implementing Project Maven, a customized AI surveillance engine that uses "Wide Area Motion Imagery" data captured by US Government drones to detect vehicles and other objects, track their motions, and provide results to the Department of Defense.

Recently, Googlers voiced concerns about Maven internally. Diane Greene responded, assuring them that the technology will not "operate or fly drones" and "will not be used to launch weapons." While this eliminates a narrow set of direct applications, the technology is being built for the military, and once it's delivered it could easily be used to assist in these tasks.

This plan will irreparably damage Google's brand and its ability to compete for talent. Amid growing fears of biased and weaponized AI, Google is already struggling to keep the public's trust. By entering into this contract, Google will join the ranks of companies like Palantir, Raytheon, and General Dynamics. The argument that other firms, like Microsoft and Amazon, are also participating doesn't make this any less risky for Google. Google's unique history, its motto *Don't Be Evil*, and its direct reach into the lives of billions of users set it apart.

We cannot outsource the moral responsibility of our technologies to third parties. Google's stated values make this clear: *Every one of our users is trusting us. Never jeopardize that. Ever.* This contract puts Google's reputation at risk and stands in direct opposition to our core values. Building this technology to assist the US Government in military surveillance – and potentially lethal outcomes – is not acceptable.

Recognizing Google's moral and ethical responsibility, and the threat to Google's reputation, we request that you:

1. Cancel this project immediately
2. Draft, publicize, and enforce a clear policy stating that neither Google nor its contractors will ever build warfare technology

Volkswagen – DieselGate (2015)

Volkswagen disclosed defeat devices and engine management software when not-for-profit researchers published results of emissions road tests. Volkswagen initially described issues as *inadvertent errors* and *rogue software engineers*.

Where were the whistleblowers in the Volkswagen emissions scandal?

September 30, 2015 4:51am BST

The emissions scandal has already taken its toll on Volkswagen. Reuters/Gaelle Ruivo

- Email
- Twitter
- Facebook
- LinkedIn
- Print

The “defeat device” used by Volkswagen to cheat emissions testing in its diesel vehicles may be history’s most costly software-related blunder.

But why did nobody in the German car giant speak out when questions were raised over how it intended to use the engine management software in some of its engines?

Rare is the whistleblower

The responsibility for the decision to deceive the emissions testers will ultimately rest some way up Volkswagen’s management chain. But as well as the senior decision-makers, there is very likely to have been a much larger group of engineers who knew of the illegal deception, understood the consequences and chose not to reveal it to authorities or the media. The lack of whistleblowers from this larger group is striking.

VW engineer jailed for emissions scandal

25 August 2017

f t e Share

Diesel emissions scandal



AFP/GETTY

Diesel Volkswagen and Audi vehicles that VW bought back from consumers sit in Pontiac, Michigan.

Vehicle Share Project - 2035

Vision

- Reduce vehicle ownership
- Network of shared vehicles
- Safer and less congested roads

Same vision, different solutions...

- A. Google
- B. Tesla
- C. DuckDuckGo
- D. UK Government Scheme
- E. Not for profit group



Group Work – 20 mins

For your allocated organisation

- Outline a solution
- Who benefits and how?
- Key priorities for the tech teams?

Group A: Google

Group B: Tesla

Group C: DuckDuckGo

Group D: UK Government

Group E: Not for profit organisation

Your organisation's solution:

- vehicles, infrastructure, connectivity
- availability, locations, end users
- technology, embedded software, apps
- scope and exclusions
- funding – who pays what


Who benefits?

Organisations with interest in project
Conflicts of interest between stakeholders
Most important stakeholders
Stakeholders with least / most power

Group Work

Priorities for your organisation's tech teams

- 3 top priorities
- 3 least priorities

1. we have freedom and creativity to produce new ideas	2. we build robust and secure software	3. we enjoy our work	4. we do not upset or annoy others
5. our software contributes to the public good	6. our software influences end users	7. we credit work of others, not taking undue credit	8. we address environmental issues
9. our work is respected	10. we are allowed to take risks	11. we raise public awareness and understanding of software	12. our software is a commercial success
13. our physical safety and well-being protected	14. our software does not discriminate against others	15. we know and apply software industry rules	16. we make our own decisions
17. we produce high quality work	18. we respect and promote principles of industry	19. we are honest and trustworthy	

Discussion....same vision, different solutions?

Differences between organisations

- Solutions
- Stakeholders
- Priorities

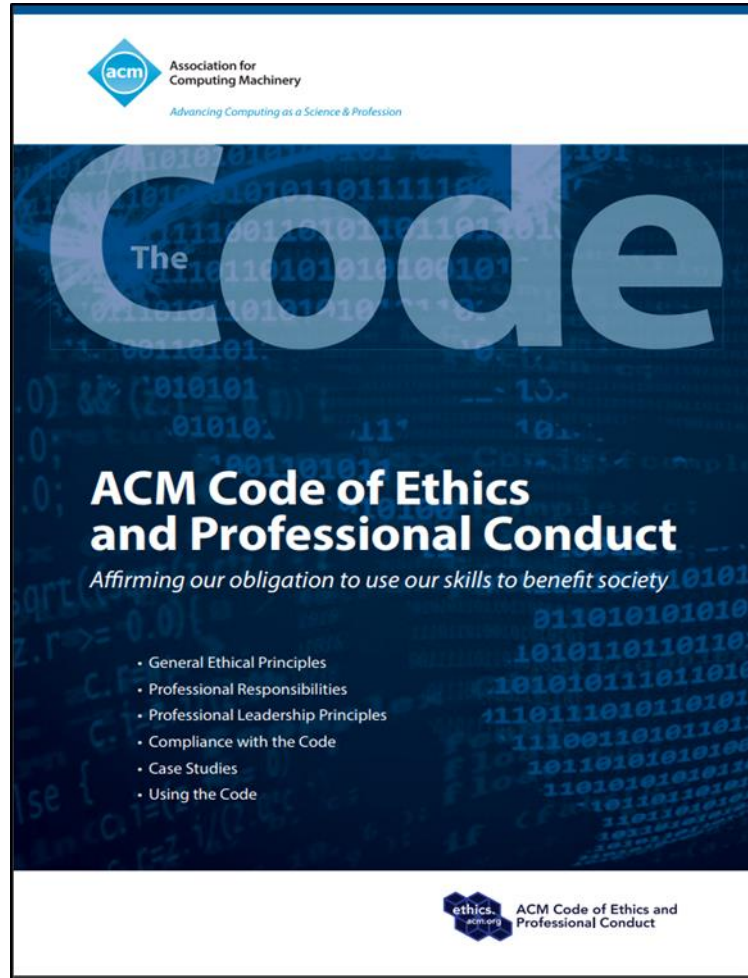
Organisation

- A. Google
- B. Tesla
- C. DuckDuckGo
- D. Government
- E. Not for profit

1. we have freedom and creativity to produce new ideas	2. we build robust and secure software	3. we enjoy our work	4. we do not upset or annoy others
5. our software contributes to the public good	6. our software influences end users	7. we credit work of others, not taking undue credit	8. we address environmental issues
9. our work is respected	10. we are allowed to take risks	11. we raise public awareness and understanding of software	12. our software is a commercial success
13. our physical safety and well-being protected	14. our software does not discriminate against others	15. we know and apply software industry rules	16. we make our own decisions
17. we produce high quality work	18. we respect and promote principles of industry	19. we are honest and trustworthy	

Where do these statements come from?

....designed to inspire and guide ethical conduct



Software Engineers
shall...

....act consistently
with the public interest

...act in the best interests of their
client and employer consistent
with the public interest

....advance the integrity and reputation
of the profession consistent
with the public interest

....temper all technical
judgments by
the need to support and
maintain human values

S#	Values Q-Sort statement (it is important to me...)	Schwartz value definition in terms of motivational goal	Schwartz value	ACM Code Statement
S1	to be given the freedom to produce new ideas, inventions & creative works	Freedom to cultivate one's own ideas and abilities	SELF-DIRECTION Thought	1.5
S2	the software I develop is robustly and usably secure	Safety and stability in the wider society	SECURITY Societal	2.9
S3	to enjoy the process of developing software	Pleasure and sense of gratification	HEDONISM	N/A
S4	that I do not annoy or upset anyone in the course of my work	Avoidance of upsetting or harming other people	CONFORMITY Interpersonal	N/A
S8	that the public good is the central concern of all professional computing work	Commitment to equality, justice, and protection of all people	UNIVERSALISM Concern	3.1
S6	that the software I develop influences the end user	Power through control of people	POWER Over People	N/A
S7	that I credit fully the work of others and refrain from taking undue credit	Recognizing one's insignificance in the larger scheme of things	HUMILITY	ACM99 7.03
S8	that I identify and address any environmental issues in my work	Preservation of the natural environment	UNIVERSALISM Nature	ACM99 3.03
S9	that my work is respected	Maintaining public image and avoiding humiliation	FACE Public Image	N/A
S10	that I am allowed to take risks when developing software	Excitement, novelty, and change	STIMULATION	N/A
S11	to improve public awareness and understanding of software	Devotion to welfare of in-group members	BENEVOLENCE Care	2.7
S12	that the software I develop is commercially successful	Power through control of material and social resources	POWER Resources	N/A
S13	that my workplace promotes my physical safety & psychological well-being	Safety in one's immediate environment	SECURITY Personal	3.3
S14	that I do not discriminate against others when developing software	Acceptance and understanding of those who are different	UNIVERSALISM Tolerance	1.4
S15	that I know and apply industry rules when developing software	Compliance with rules, laws and formal obligations	CONFORMITY Rules	2.3
S16	that I make own decisions when developing software	Freedom to determine one's own action	SELF-DIRECTION Action	N/A
S17	that I personally achieve high quality in software design and production	Success according to social standards	ACHIEVEMENT	2.1
S18	to uphold, promote and respect the principles of my industry	Maintaining & preserving cultural, family or religious traditions	TRADITION	4.1
S19	to be an honest and trustworthy colleague	Being a reliable and trustworthy member of the in-group	BENEVOLENCE Dependable	1.3

Applying Human Values Theory to Software Engineering Practice: Lessons and Implications.

Ferrario, Maria Angela; [Winter, Emily](#). In: IEEE Transactions on Software Engineering, Vol. 49, No. 3, 01.03.2023, p. 973-990.

There's no one type of software engineer...

We are carrying out exercises with software engineers in industry, research and the public sector and have found the following types...

- **Type 1:** Socially-concerned, intrinsically motivated
- **Type 2:** Autonomous, non-conforming risk-taker
- **Type 3:** Fun-loving, extrinsically motivated

Evil Twin... 10 minutes in your team

What might happen on your project and why?

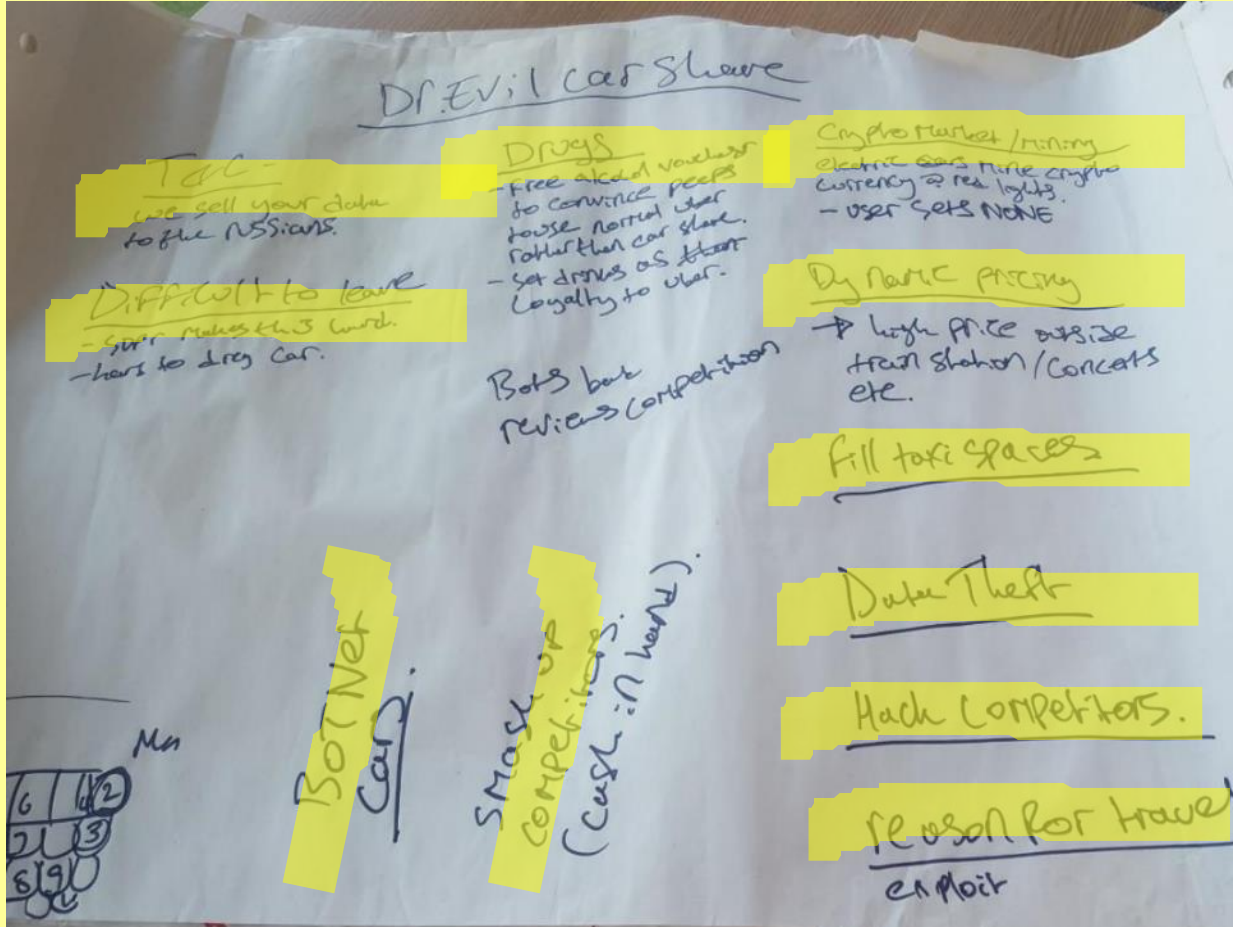
- What hidden agendas might stakeholders have?
- What hidden agendas might delivery teams have?
- What might the delivery team do (or be asked to do) and why?
- Who might find malicious ways to use or misuse your system?
- What vulnerabilities might the system have?
- Who benefits / loses from the evil twin?



(Poor practices, negligence, accidental or intentional harm)

Group Discussion

What can we learn from these extreme misuse cases?



How to turn negatives into positives?

Dr Evil:

- Crypto mining
- Dynamic pricing
- Block taxi spaces
- Data theft
- Sell your data
- Be difficult to leave
- Hack competitors
- Exploit travellers
- Botnet cars



How would you prevent, deter or detect "evil" things happening on your projects?
How might your value priorities change?