VALUE SENSITIVE DESIGN: CYBERSECURITY

Kevin Mills

February 27, 2020

Northeastern University

CAMBRIDGE ANALYTICA

CAMBRIDGE ANALYTICA IN A NUTSHELL

https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

- Cambridge Analytica attained data for ~87 million Facebook users.
    - “hundreds of thousands” of Facebook users were paid to take a survey that would collect data “for academic use”
    - Because of how Facebook handled privacy permissions, the app was able to collect data not just from those who installed and used it, but also *from all their friends*.
    - Facebook’s “platform policy” allowed the use of friends’ data to “improve user experience in the app and barred it being sold on or used for advertising”
- Cambridge Analytica used this data to construct “psychographic profiles” of users.
- They used these profiles to target political advertisements, thus influencing the 2016 presidential election.

CAMBRIDGE ANALYTICA

Dr Alex Kogan [redacted] 9 May 2014 at 02:14
To: Christopher Wylie [redacted], [redacted]

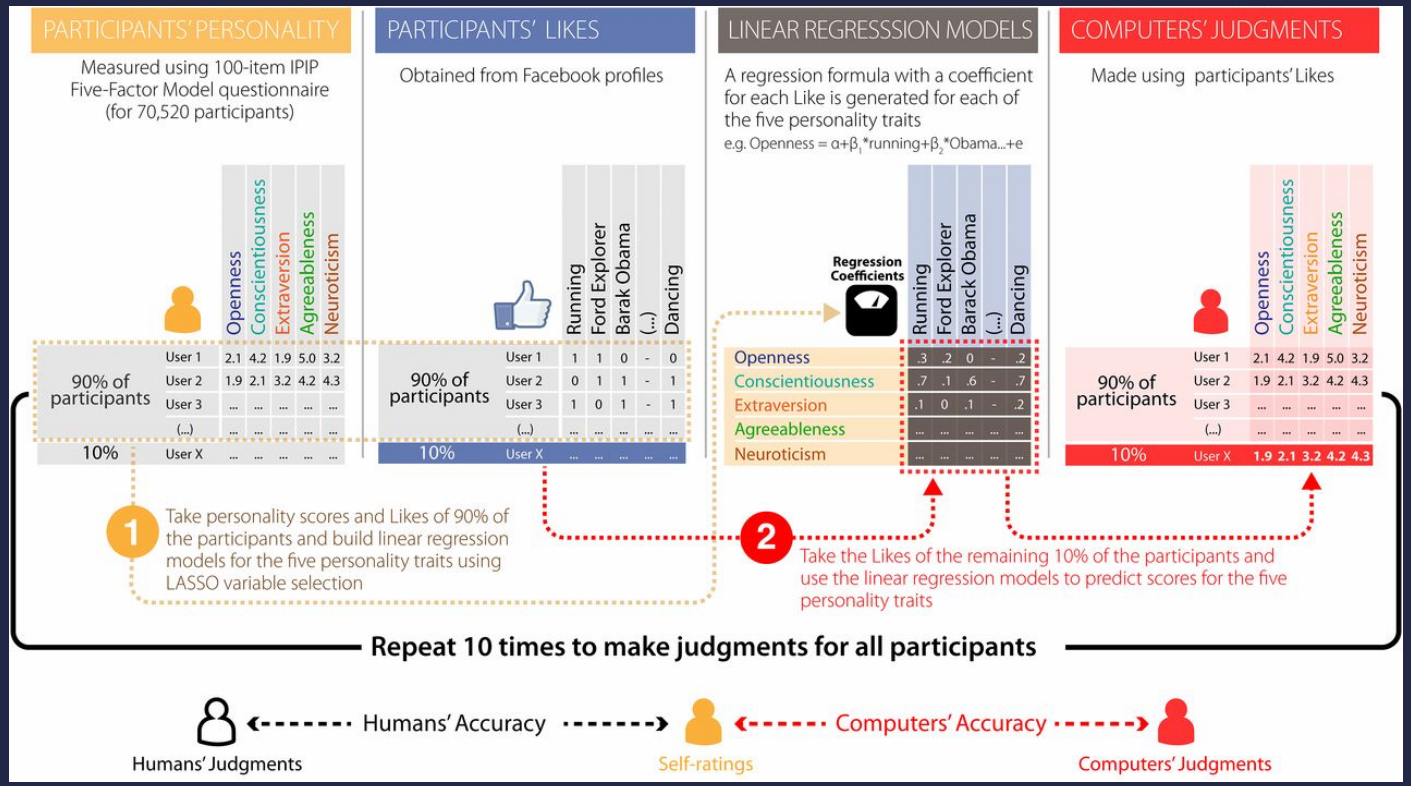
Hey Chris and [redacted],

Great chatting with you both yesterday. Here is a list of traits that can be predicted now--good starting shopping list. More specific items can also be predicted within the bigger personality questionnaires, but this is a start to get you thinking about what you may want:

- openness
- conscientiousness
- extraversion
- agreeableness
- neuroticism
- life satisfaction
- iq
- gender
- age
- political views = conservative?
- political views = liberal?
- political views = uninvolved?
- political views = libertarian?
- religion (categorical)
- job (categorical)
- university subject concentration (categorical)
- self-disclosure (do you tell people about yourself or not?)
- fair-mindedness (fair or suspicious in dealings with others?)
- self-monitoring (do you change your personality depending on who you're with)
- sensational interests (has 5 factors, "militarism" [guns and shooting, martial arts, crossbows, knives], "violent occultism" [drugs, black magic, paganism], "intellectual activities" [singing and making music, foreign travel, the environment], "credulousness" [the paranormal, flying saucers], "wholesome interests" [camping, gardening, hill-walking], see: https://www.academia.edu/157864/The_first_sensational_interests_paper - it's used in forensic psychology to understand criminality)
- belief in star signs (5 point scale)

DATA MINING

Wu Youyou, Michal Kosinski, and David Stillwell (2015) studied how well they could predict personality traits based on data from Facebook “likes”.



DATA MINING

"Compared with the accuracy of various human judges reported in the meta-analysis (20), computer models need 10, 70, 150, and 300 Likes, respectively, to outperform an average work colleague, cohabitant or friend, family member, and spouse (gray points)." (Youyou et al., 2015)

"How accurate is the computer, given an average person? Our recent estimate of an average number of Likes per individual is 227 (95% CI = 224, 230),‡ and the expected computer accuracy for this number of Likes equals $r = 0.56$. This accuracy is significantly better than that of an average human judge ($z = 3.68$, $P < 0.001$) and comparable with an average spouse, the best of human judges ($r = 0.58$, $z = -1.68$, $P = 0.09$). The peak computer performance observed in this study reached $r = 0.66$ for participants with more than 500 Likes. The approximately log-linear relationship between the number of Likes and computer accuracy, shown in Fig. 2, suggests that increasing the amount of signal beyond what was available in this study could further boost the accuracy, although gains are expected to be diminishing." (ibid.)

DATA MINING

"We show that easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. The analysis presented is based on a dataset of over 58,000 volunteers who provided their Facebook Likes, detailed demographic profiles, and the results of several psychometric tests. The proposed model uses dimensionality reduction for preprocessing the Likes data, which are then entered into logistic/linear regression to predict individual psycho-demographic profiles from Likes. The model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases." (Kosinski et. al, 2013)

SOME BAD SECURITY CHOICES

- Facebook insists that there was no *technical* failure in their security procedures.
    - They were not hacked.
- But the scandal arguably reveals that the security procedures themselves were flawed.
    - Why were apps able to access the data not just of those who installed them, but also of all their friends?
    - Why was crucial user data secured merely by a policy requirement in the “platform policy” and not technically?
    - Was it clear to users that privacy on Facebook worked that way?
        - (It might be now; it definitely wasn’t at the time, at least in general.)

GOOGLE’S “PROJECT ZERO”

WHAT IS PROJECT ZERO?

“Formed in 2014, Project Zero is a team of security researchers at Google who study zero-day vulnerabilities in the hardware and software systems that are depended upon by users around the world. Our mission is to make the discovery and exploitation of security vulnerabilities more difficult, and to significantly improve the safety and security of the Internet for everyone.

We perform vulnerability research on popular software like mobile operating systems, web browsers, and open source libraries. We use the results from this research to patch serious security vulnerabilities, to improve our understanding of how exploit-based attacks work, and to drive long-term structural improvements to security.”

(https://googleprojectzero.blogspot.com/p/about-project-zero.html)

WHAT IS PROJECT ZERO?

FROM THEIR FAQ

“When Project Zero finds a new vulnerability, we send a detailed technical description of the issue to the relevant vendor or open source project. This initial vulnerability report includes the following statement:

"This bug is subject to a 90 day disclosure deadline. After 90 days elapse or a patch has been made broadly available (whichever is earlier), the bug report will become visible to the public."

Our expectation is that the developer will fix the security vulnerability within 90 days. Project Zero won't publicly discuss details about the vulnerability until the issue has been fixed, or until 90 days pass without a patch being made available to users, whichever is earlier.”

(https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html)

WHAT IS PROJECT ZERO?

FROM THEIR FAQ

“What proportion of vulnerabilities are fixed before the 90-day deadline?

As of July 30, 2019 we have 1585 vulnerabilities in a "Fixed" state in our issue tracker, and 66 vulnerabilities have been disclosed without a patch being available to users. That means that over the total lifetime of Project Zero, 95.8% of issues have been fixed under deadline.

If we limit the analysis to the time period where grace extensions were an option (Feb 13, 2015 to July 30, 2019) then we have 1434 fixed issues. Of these, 1224 were fixed within 90 days, and a further 174 issues were fixed within the 14-day grace period. That leaves 36 vulnerabilities that were disclosed without a patch being available to users, or in other words 97.5% of our issues are fixed under deadline.”

(https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html)

WHAT IS PROJECT ZERO?

FROM THEIR FAQ

Why are disclosure deadlines necessary? (Excerpts)

“We were concerned that patches were taking a long time to be developed and released to users, and we felt that disclosure deadlines set up the right balance of incentives.”

“We can't know for sure when a security bug we have reported has previously been found by an attacker (recent attempts to quantify the rate of bug collision can be found here and here), but we know that it happens regularly enough to factor into our disclosure policy. We think that our policy introduces an appropriate level of urgency into the vulnerability remediation process.”

“While every vulnerability disclosure policy has certain pros and cons, Project Zero has concluded that a 90-day disclosure deadline policy is currently the best option available for user security. Based on our experiences with using this policy for multiple years across hundreds of vulnerability reports, we can say that we're very satisfied with the results. No one on Project Zero is happy when a deadline is missed, but a consistent and fair approach to enforcing disclosure deadlines goes a long way.”

(https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html)

SOME ETHICAL QUESTIONS ABOUT PROJECT ZERO

(THE ANSWERS MAY BE THAT GOOGLE DOES NOTHING WRONG HERE, AND INDEED, PROVIDES A VALUABLE PUBLIC SERVICE – BUT IT'S IMPORTANT TO THINK THIS THROUGH!)

1. Do they have a right to do this?
    1. Is it fair to threaten software producers with public disclosures of their vulnerabilities, thus forcing them to implement potentially costly fixes on a schedule Google deems to be reasonable?
        1. How hard is it to fix these vulnerabilities once they are disclosed?
    2. Is this fair to users of the relevant software, who may be vulnerable if software developers fail to fix the problem before Google discloses it?
        1. Of course, is it fair to users if these vulnerabilities exist and *aren't* addressed?
2. Does this project, on balance, have good consequences?
    1. Were discovered vulnerabilities likely to be exploited anyway?
    2. Are Google researchers better at determining security priorities than the original software developers?
3. What are Google's motives in funding this? How, if at all, does this effect the operations of Project Zero?

LAW AND MORALITY

LAW VS MORALITY

LAW VS MORALITY

LAW VS MORALITY

- What is legal is not necessarily moral.
- What is illegal is not necessarily immoral.
    - Although in a just society, you should almost always follow the law.
- Legal compliance should be thought of as the minimum standard for responsible conduct.
    - This is especially true for emerging technology fields, where legal standards may be poorly developed.
- It’s important to think not just about what’s *legal* and *illegal*, but what’s *moral* and *immoral*.

ETHICS, MORALS, VALUES

WHAT IS ETHICS?

Morals: specifications of how we ought to live our lives.

Ethics: the study of morals.

> ("Morals" and "Ethics" are often used as synonyms, but this is one way of understanding them)

Descriptive Ethics: studies people's *beliefs about* morals (typically a specific group of people).

Normative Ethics: studies morals themselves, i.e. not what people believe about how we should live our lives, but how we actually should live our lives.

NORMATIVE ETHICS

Are there answers to questions about how we ought to live?

In many cases, there probably aren't uniquely right answers.

- It may be that multiple answers are reasonable.

But there are definitely lots of wrong answers.

- E.g. there are interesting questions about how long Google should give software producers to fix vulnerabilities found by Project Zero.
    - But immediately disclosing the vulnerability without any notice is clearly the wrong way to go.

NORMATIVE ETHICS

Are there answers to questions about how we ought to live?

There may not be uniquely right answers.

Even if there are uniquely right answers, it might be very difficult to find out what these are.

All things considered, there is no simple algorithm for ethics.

- You have to pay attention to the particularities of the situation – e.g. what values are relevant, and for which stakeholders – and use your judgment to determine how to proceed.

CYBERSECURITY ETHICS

VALUES AND TECHNOLOGY

Technology is the result of human imagination

All technology involves design

All design involves choices among possible options

All choices reflects values

Therefore, all technologies reflect and affect human values

Ignoring values in the design process is irresponsible

Engaging with values in the design process offers creative opportunities for:

- Technical innovation
- Improving the human condition (*doing good* and *saving the world*)

VSD IN ACTION: SOME CORE COMPONENTS

1. Identify stakeholders.
2. Identify the values at stake for these stakeholders.
3. Identify where value tradeoffs are necessary.
4. Prioritize important values.
5. Use this to define success.

VALUE SENSITIVE DESIGN: DEFINING SUCCESS

One of the most important parts of value sensitive design is finding the right definition of “success” for your project.

Projects with bad success definitions may succeed on their own terms, but be very bad in other respects.

A good success definition should reflect the values and stakeholders that are at play for the technology in question.

VALUE SENSITIVE DESIGN: DEFINING SUCCESS

The success definition for cybersecurity is in some sense “security”, but…

- What exactly does this mean?
  - What is security and why is it important?

- How much security is desirable?
  - Security typically involves costs
    - “maximal” security is probably neither possible nor desirable
  - Security is fundamentally about *risk management*
    - i.e. allocating appropriate resources to maintain reasonable albeit imperfect security.

WHY IS CYBERSECURITY IMPORTANT?

Value: something that is *important*, i.e. bears on how we ought to live.

Intrinsic value: something that is valuable for its own sake.

Instrumental value: something that is valuable only as a means for getting something else.

What is the value of cybersecurity?

- Is it intrinsically valuable?
- Is it instrumentally valuable?
    - If so, what is it instrumentally valuable for?

WHY IS CYBERSECURITY IMPORTANT?

SOME INSTRUMENTAL VALUES

(WITH HELP FROM VALLOR AND REWAK, 2017)

- Privacy
  - Identity theft
  - Blackmail, extortion
  - Espionage (corporate or government)
  - Embarrassment
- Property
  - Intellectual property
  - Bank accounts
- System Function
  - Cybersecurity keeps systems functioning
  - Cybersecurity is thus valuable for all the reasons the systems that depend on it are valuable
    - E.g. in a healthcare context, cybersecurity is valuable because it promotes health
    - Understanding the values that are at stake in cybersecurity thus requires an understanding of the concrete system under consideration. This can’t be done completely in the abstract.

STAKEHOLDERS IN CYBERSECURITY

- Understanding the value of cybersecurity is a good start on understanding the values that are relevant *to* cybersecurity.
  - But it is only the start.
- When thinking about the values relevant to your project, it can be useful to think about whose values / interests are affected by the technology in question.
- These are the stakeholders.
  - Direct stakeholders: users, producers, and owners of the technology in question.
  - Indirect stakeholders: people who do not directly interface with the technology in question, but are affected by it nonetheless.
    - The distinction is really just a heuristic; the basic point is to recognize that technology affects more than just the people who themselves use it.

STAKEHOLDERS: DIRECT AND INDIRECT

- Direct stakeholders:
  - Producers of the technology
    - Their financial backers
  - Users of the technology

- Indirect stakeholders:
  - Needs to be assessed on a case-by-case basis
    - May include people whom the system is used on behalf of
      - E.g. patients in a healthcare system
    - May include the public at large, or some subset of them.

STAKEHOLDERS IN CYBERSECURITY

Example 1: Facebook and Cambridge Analytica

Who are the stakeholders?

- Direct Stakeholders:
  - Facebook
  - Users of Facebook
  - Cambridge Analytica
- Indirect Stakeholders:
  - American citizens
    - (Because Facebook's data was ultimately used to try to influence an election)

STAKEHOLDERS IN CYBERSECURITY

Example 1: Facebook and Cambridge Analytica

What's at stake for these stakeholders?

- Direct Stakeholders:
  - Facebook
    - Money + Reputation
  - Users of Facebook
    - Privacy
    - Autonomy
  - Cambridge Analytica
- Indirect Stakeholders:
  - American citizens
    - Democracy

STAKEHOLDERS IN CYBERSECURITY

Example 2: Project Zero

STAKEHOLDERS IN CYBERSECURITY

Example 2: Project Zero

Who are the stakeholders?

- Direct stakeholders:
  - Producers of the software with the vulnerability
  - Users of the software with the vulnerability

- Indirect stakeholders:
  - Google

STAKEHOLDERS IN CYBERSECURITY

Example 2: Project Zero

What's at stake for these stakeholders?

- Direct stakeholders:
  - Producers of the software with the vulnerability
    - Money / Reputation
    - Resources / Opportunity costs
  - Users of the software with the vulnerability
    - Hard to know without knowing more about the system in question…
      - Privacy /Property
      - System integrity
      - Money and opportunity costs (?)
- Indirect stakeholders:
  - Google
    - Wants people to use online services
      - They profit from this
    - Potentially hurts a competitor
      - Hopefully this isn't motivating them, but this looks like something that's at stake.

VALUE TRADEOFFS

- Value tradeoff: when two values, each of which is important, are to some extent mutually incompatible, and a balance must be struck between them.
  - Sometimes this might be different values had by the same party.
    - E.g. a producer who values security but also resource efficiency.
  - Sometimes it might be the same value held by different parties.
    - E.g. my financial interests and the technology producer's financial interests.
- Doing cybersecurity in a morally appropriate way means striking the (morally) right balances between all these conflicting values.
  - This is hard!

VALUE TRADEOFFS

- Given that cybersecurity is fundamentally about risk management, it will unavoidably involve value tradeoffs.
- Moreover, different stakeholders (e.g. producers, users, and users-by-proxy) may want different things when it comes to cybersecurity
  - Broadly speaking, they all want systems to be secure, but what's at stake can differ significantly
    - As a result, they may disagree on how *much* security is worth it
  - Producers typically have their reputation and relationship with users at stake
  - Users and/or users-by-proxy may have much more at stake
    - E.g. in a health context, users-by-proxy may literally have their lives at stake.
    - In a financial context, users may be subject to theft or identity theft in a financial breach.

VALUE TRADEOFFS

- There may be no uniquely right answer when dealing with value tradeoffs, and even if there is a uniquely right answer, it may be very difficult to find.
  - Plenitude Cases
    - Example 1: you love programming and you love math; there may be no unique answer as to whether you should be a programmer or a mathematician.
  - Tragedy Cases
    - Example 1: “Sophie’s choice”, where a mother is forced to choose which of her children will live and which will die.
    - Example 2: Your company is the victim of ransomware, which has locked you out of (and threatens to irretrievably damage) user data.
    - Example 3: Your loved one asks you about an outfit which, as a matter of fact, they really don’t look great in.
      - A mild tragedy, admittedly.

VALUE TRADEOFFS

- Value tradeoffs are difficult and there is no mechanical algorithm for how to make them properly.
- But the following steps should help guide you:
  - Assess legitimacy.
    - Sometimes somebody's values are *illegitimate* and don't count at all in a given context.
      - For example, a burglar has a financial interest in you leaving your home unlocked.
  - Respect rights
    - There are certain values you *must* respect, or must respect unless something very serious is on the line.
      - E.g. no matter how much money you can make, you can't …
  - Promote stronger values.
    - E.g. there is currently a value tradeoff between maximizing profit and preserving the environment.
    - Preserving the environment surely wins here.
      - It's not that the economy is unimportant; it's that preserving a habitable planet is *far more* important.

VALUE TRADEOFFS

- What follows are some assessments of the value tradeoffs in the Cambridge Analytica and Project Zero cases.
- Note that these matters are not black and white!
- This is one way of analyzing these scenarios, but I don't mean to suggest it's the only way, or that these analyses are unequivocally "the answers".
    - Value Sensitive Design is a heuristic framework to help you think about moral issues, not an easy and unequivocal source of answers.

STAKEHOLDERS IN CYBERSECURITY

Example 1: Facebook and Cambridge Analytica

What's at stake for these stakeholders?

- Direct Stakeholders:
  - Facebook
    - Money + Reputation
  - Users of Facebook
    - Privacy
    - Autonomy
  - Cambridge Analytica
- Indirect Stakeholders:
  - American citizens
    - Democracy

STAKEHOLDERS IN CYBERSECURITY

Example 1: Facebook and Cambridge Analytica

What's at stake for these stakeholders?

- Direct Stakeholders:
  - Facebook
    - Money + Reputation
      - These are legitimate interests, but not as important as the others.
  - Users of Facebook
    - Privacy
      - Users arguably have a (moral) right to privacy, and this can't justly be violated for profit.
    - Autonomy
  - ~~Cambridge Analytica~~
    - Cambridge Analytica was a bad-actor in this scenario, and their interests can be ignored.
- Indirect Stakeholders:
  - American citizens
    - Democracy
      - This is also an extremely strong value (arguably a right) that needs to be respected.

STAKEHOLDERS IN CYBERSECURITY

Example 2: Project Zero

What's at stake for these stakeholders?

- Direct stakeholders:
  - Producers of the software with the vulnerability
    - Money / Reputation
    - Resources / Opportunity costs
  - Users of the software with the vulnerability
    - Hard to know without knowing more about the system in question…
      - Privacy /Property
      - System integrity
      - Money and opportunity costs (?)
- Indirect stakeholders:
  - Google
    - Wants people to use online services
      - They profit from this
    - Potentially hurts a competitor
      - Hopefully this isn't motivating them, but this looks like something that's at stake.

STAKEHOLDERS IN CYBERSECURITY

Example 2: Project Zero

What's at stake for these stakeholders?

- Indirect stakeholders:
  - ~~Google~~
    - Wants people to use online services
      - They profit from this
    - Potentially hurts a competitor
      - Hopefully this isn't motivating them, but this looks like something that's at stake.
  - Neither of Google's direct interests is legitimate in this context. If their motive with Project Zero is to profit or to hurt a competitor, then they are effectively engaging in extortion.
  - The justification for Project Zero must thus not derive from profit, but must be altruistic: to help secure the internet for the sake of others.
    - Of course, it's fine if Google ends up benefiting from this too.

STAKEHOLDERS IN CYBERSECURITY

Example 2: Project Zero

What's at stake for these stakeholders?

- Direct stakeholders:
  - Producers of the software with the vulnerability
    - Money / Reputation
    - Resources / Opportunity costs
  - Users of the software with the vulnerability
    - Hard to know without knowing more about the system in question…
      - Privacy /Property
      - System integrity
      - Money and opportunity costs (?)
  - Absent more details, it's hard to assess how to do value tradeoffs here. Both parties have legitimate interests here.

VALUE TRADEOFFS: FREE MARKET TO THE RESCUE?

- Given that:
  - Cybersecurity inevitably involves value tradeoffs (it's fundamentally about risk management)
  - There may be no unique answers in matters involving value tradeoffs
    - And even if there are, they can be very hard to find

- The question arises:
  - Who should get to make decisions about value tradeoffs in cybersecurity?

- One possible answer is: leave it to the market.
  - Producers of technology are free to decide how much to spend on security.
    - And will bear serious costs if they make bad decisions.
  - Users of technology can decide for themselves whether a platform is secure enough for them to use.

VALUE TRADEOFFS: FREE MARKET TO THE RESCUE?

- There are some worries for this approach, because there are significant power asymmetries between producers and users of technology.
    - Information asymmetries: many users and users-by-proxy don't understand the security features or implications of the systems they use.
    - Power asymmetry: many users, and especially users-by-proxy, may have little or no control over the systems they have to use.
        - Or at least: not enough control to bargain from a fair position.
- In short, users and users-by-proxy are vulnerable to security breaches, and may lack the information and power to protect themselves.

VALUE TRADEOFFS: FREE MARKET TO THE RESCUE?

- Cybersecurity professionals may have a duty of care to users of technology.
  - This is common with professionals.
    - Doctors are expected to care for patients' health
    - Lawyers are expected to care for clients' legal needs
    - Teachers are expected to care for students' education needs

- Cybersecurity researchers might owe it to users, as a matter of ethics, to make their platforms secure.
  - And given the power and information asymmetries involved, it isn't good enough to say "let users decide how much security they want".
- Exactly how much security is required is once again a tricky question.
  - But the mere fact that users have "agreed" to the risks associated with some security vulnerability does not entail this is fair.

VALUE TRADEOFFS: FREE MARKET TO THE RESCUE?

- Project Zero is presumably supposed to help with this.
  - The assumption seems to be that producers of technology are either inadequately incentivized to promote the security of their products, or lack the resources to do so, and that users are vulnerable because of this.
    - There seems to be good evidence that this does happen.
  - Project Zero can then help (and force) technology producers to better secure their systems, thus protecting users who may not know enough or have the power to protect themselves.

- Some questions …
  - Are producers of technology inadequately incentivized to promote security?
  - Is this a market failure that needs to be addressed somehow?
  - Does Google's *Project Zero* address this market failure?

A QUICK NOTE ON PROFESSIONAL ROLE OBLIGATIONS

- Cybersecurity professionals may occupy a variety of competing roles.
  - For example, a cybersecurity professional might be hired to do a security audit, and expressly told only to disclose what is found to the company in question.
- Understanding the professional role of cybersecurity researchers is complicated, and at the moment, perhaps not fully well-defined.
  - Edward Snowden decided that his obligations to his employer – the NSA – were outweighed by his obligations to the public to disclose the NSA's surveillance projects.
    - Whether this was morally justified is a tricky question.
- But understanding your role can help you understand how to deal with value tradeoffs.

VSD FOR CYBERSECURITY

- Again, there are no easy answers here, and there is *no algorithm*.
  - But doing the following should help provide guidance.
- Identify the relevant stakeholders.
  - Both direct and indirect.
- Identify the values that are relevant to those stakeholders.
- Understand your professional role.
  - It's likely that you owe a duty of care to users / users-by-proxy of your system.
  - But you may be in a context in which certain courses of action are inappropriate.
- Formulate a success definition that strikes appropriate tradeoffs.
- Do your best to achieve success, as defined.
- Forgive yourself if you make mistakes, but make a sincere effort to get cybersecurity right.

IN-CLASS EXERCISE: A CASE OF YOUR OWN

Consider Edward Snowden's dilemma.

- He discovered a significant surveillance apparatus that was gathering information on American citizens without warrants.
- He ultimately concluded he had a moral obligation to disclose this to the public, and did so.
- In doing so, he made the public aware of this apparatus.
- But disclosing the existence of this apparatus arguably hindered its ability to catch terrorists and bad actors.

Some helpful things to think about:

1. Identify stakeholders.
2. Identify the values at stake for these stakeholders.
3. Identify where value tradeoffs are necessary.
4. Prioritize important values.
5. Use this to define success.