Data and Goliath

Bruce Schneier

Chapter 12&13

Juho Juvani

21.4.2016

CT60A7001 Critical Thinking and Argumentation in Software Engineering

LAPPEENRANTA UNIVERSITY OF TECHNOLOGY

Chapter 12: Principles

Security and Privacy

- Author echoes words of Solove: Security versus Privacy is a false trade-off
- Not all security, for example, impinges on privacy.
  - Door locks, tall fences, guards, reinforced doors, etc.
- Second point made: Privacy and security go hand in hand.

  → Without privacy people feel exposed and vulnerable – less secure.
- The Fourth Amendment says ”the rights of the people to be secure in their persons, houses, papers and effects”
- This is a clear indication that privacy, according to the author, is fundamental to the security of the individual.
- We return to the thinking of ethics – exactly, the principles of doing something. What do you think?

Security and Privacy 2

- How much would you pay for privacy?
- How much would you pay for security?

- Both questions are misleading, and false trade-off's, again.
- Lack of security is a very real and visceral, whereas lack of privacy can only be truly felt when faced with the aftermath of the breach.

- Author argues that using events like 9/11, and life-threatening threats as a trade-off for loss of privacy is at best theoretical.
  - Can only at best reduce the chance of new 9/11 with very small marginal, for the chance is already extremely small in.
- Goal should be to maintain both together, not trade one for the other, or find acceptable excuses to do so.

Security over surveillance

- System build for security is harder to surveil
- System build for easy surveillance is harder to secure
- Should backdoors and surveillance be allowed, when there is no way to guarantee that only the ”right” people can use it, or should all exploits be blocked?
- Author makes an excellent argument :
  - ”It rains on the just and unjust” – all we have can be used for both good and bad. Nothing is just meant for ”one thing” – People are the ones that use the tools.
  - Because of this, we should side with security, because percentage of bad is so negligible in comparison to majority.

Security over surveillance 2

- Example 1:
  - Tor – free open-source software for anonymous internet browsing. First developed by US Naval Research Laboratory, then State Department.
  - Now NSA and FBI are both trying to crack it. China is trying to ban it, and at the same time all use it to keep anonymous. It shows that it's either strong enough to protect anonymity of all, or none at all.
- Example 2:
  - Airplane security is extreme example, designed with minority evil in mind. Reason:
    - The chance of failure has potentially catastrophic consequences compared to anything else.
- Package tracking is easy example of surveillance system. Very open and transparent system.
- General principle with security versus surveillance: Systems should be designed with minimal surveillance necessary for them to function.

Transparency

- Trust comes from transparency
- For personal data: People should be entitled to know what data is being collected about them, what is archived, and how it is used – and by whom.
- These days we also need to know where, in which country, it is being stored at.

- Since we do not know algorithm that is used to select people for ”special screening” in customs, for example, can we judge it’s fairness?

- What about other hidden algorithms? Google search? Tinder matchmaking?

Transparency 2

- Author argues that transparency is a good thing to aim, whenever possible.
- Is it good thing we have become so transpared, as to air all our daily events, worries, relationship status and even really awkward situations online?

Oversight and accountability

- Social contract of democracy degrees that we have to give power over ourselves to others. The only way to do this safely is if we have trust that this power is not abused, and that we can punish those that do.

- Two levels of oversight: Strategic and Tactical
  - Strategic: Are rules we're imposing the correct ones?
    - Procedures should ensure the rules are followed, but no agency should be able to decide what rules it should follow.
  - Tactical: Are the rules being followed?
    - The correct processes and regulations should enforce the rules – do they?

Oversight and accountability 2

- Different organizations should provide tactical oversight of one another. For example:
  - The police require a warrant to be granted by a neutral third party – a judge – who is taked to ensure that rules are followed.
- Tactical and Strategic oversight is difference between doing things right and doing the right things. These powers should not be abused.
  - This is why accountability is needed.
- Author reminds us of three things to remember for a good balance: ”Transparency, oversight and accountability.”

Principle of resilient design

- There is no perfect system
- Imperfections have to be accepted and acknowledged
- Everything should be designed to expect these imperfections, so that we can predict the failings.
- This is what is called resilience.

Chapter 12 conclusion

- Our communication infrastructure can either be:
  - Secure or not
  - Private or not
  - It can be open to surveillance or not
  - It can be resilient or not

- Whatever is decided, everyone will be able to use that infrastructure and that should be kept in mind.
- There is no option to only guarantee that ”good guys” can use something – it will be available for both the good and bad.

Chapter 13: Solutions for Government

So what are the solutions to all these past issues, and what can we do to meet these principles?

More transparency and less secrecy

- Police has a lot of transparency in its work, rules and processes.
  - Individuals and names are kept secret
  - Processes and general knowledge of ”what” and ”how” they do things, is known though.
  - Does not deter the police from making arrests and regularly solving crimes.

- Author notes that terrorists are not smarter, more formidable nor do they kill or damage more people than organized crime.
- So question is: What excuse does NSA or any organization have for the excessive secrecy in counter-terrorism?

More – and better – oversight

- Declassified documents have shown that NSA has not, actually, followed the the letter of the law as they claimed in past.
- This proves that rules are being gamed
- There is full disclosure – in closed rooms, allowed only for top-secret security clearance
  - → Only rare few have access to all of the necessary information, and even less has expertise required to understand it
  - → How exactly can oversight happen when all is not understood?

- Is there any reason why organization like NSA should not be more transparent, or have clear and more transparent oversight?

Protect whistleblowers

- The author makes an argument for protecting whistleblowers and journalists from espionage charges
- In the case where information is leaked in conscience-driven disclosure of official wrongdoing, there should be a chance for the court to make a decision on the accusations and individual in question.

- What do you think about treating journalism as a crime when secret information is revealed? Like in Snowden’s case.
- What about when it reveals clear misconduct or blatant wrongdoings?

Target narrowly, and only with judicial approval

- Surveillance should require warrants and oversight, whether it’s emails, papers at home, computer at work or even Google’s search history.

Vulnerabilities and subverting products

- Systems and products should fall and stand on their own merits
- Governments should stop hoarding and gathering vulnerabilities, and stop demanding ”sabotage” of existing systems with backdoors or intentional exploits.
- Vulnerabilities are not one sided, they are available for all
  - → They should be fixed

- Author makes argument for national and global trust for products, brands and reputation of service.
  - Mistrust becomes poison, and added doubt brews more hostility

- What do you think about designing systems with backdoors or exploits?

NSA and military

- NSA should be separated from the domestic surveillance, and have it's responsibilities returned to prior the 9/11.
  - Focus on espionage against foreign governments
  - Only targeted counter-terrorism with supervision
  - Pursue leads based on expertise of the FBI, not the surveillance databases

- Military actions online should be supervised and limited carefully.
  - War is war, whether it's real life or in cyberspace
  - Attacks in cyberspace should be done with intention of real military action, not as an act of espionage – These two must be separated
  - Military actions in cyberspace should require approval at the highest levels of executive branch

Finally

- Author suggests support for a free, open, and global internet with common, decentralized areas and places.
- First amendment protects freedom of speech in public spaces, and this is also how we view online discussion.
- Modern world benefits from the global connection, and people expect it to be their right to have that freedom even through facebook discussion

- Unfortunately, facebook, twitter, etc. Are all considered private space, so laws do not apply to them.
  - User agreements even takes away any right to appeal or complain.

- Should similar laws to freedom of speech and privacy be included to online spaces? Even limitations, like drunkness and lewdness, as author mentions?

Thank you for listening