NTNU
Kunnskap for en bedre verden

Department of ICT and Natural Sciences

IDT8000 - Research Ethics

Implementing Zuboff's shout into code

Author:
Luka Grgičević

April, 2022

Table of Contents

1 Introduction

This survey outlines what privacy and software developers have in common. It also encapsulates a bigger story about surveillance capitalism and the Privacy by Design framework which is trying to be incorporated today. A brief description of Shoshana Zuboff's work during the recent years and references therein is presented in the second chapter, while the third chapter examines what is being done today throughout the software developers community as recently presented in Mohammad Tahaei's PhD thesis and references therein.

2 Privacy

Since the dawn of life, a being gathers information from his consciousness and processes them through thoughts and stores that information as factual knowledge. As we move through life, we analyse that data and form unique behaviours. Common knowledge is what our continuously gathered information from surroundings entangles and has a common ground with other being's cognition. Via the scientific method, common knowledge may become the fact that we may hold on to. The core of our knowledge about ourselves is something we build over time and something we certainly don't profoundly know about but drives our autonomy or self-governance, which implies living according to one's own reasons. We can build up what privacy might be from now on.

2.1 Definitions

As Dorota Mokrosinska recently wrote: ”Privacy protects autonomy by protecting the social contexts which make the exercise of individual autonomy meaningful.”, and: ”Privacy is a condition of autonomy because it enables individuals to control what information about them can and cannot be accessed and collected. Without such control, self-governance is impossible.” [5]

She also stated: ”Social roles and practices create and provide a social framework in which the exercise of autonomy becomes meaningful. By regulating social roles, practices and relations, privacy facilitates the social conditions of the meaningful exercise of autonomy. Privacy is also necessary for the constitution of social roles, relationships and social practices (that make the exercise of autonomy possible).”

Judge Richard Posner views privacy as giving individuals “power to conceal information about themselves that others might use to (the individual's) disadvantage.” [9]

Legal scholar Fred Cate declares that privacy is “an antisocial construct...(that) conflicts with other important values within the society, such as society's interest in facilitating free expression, preventing and punishing crime, protecting private property, and conducting government operations efficiently.” [3]

On the other hand, practising autonomy might be harmful to ourselves, so concessions must be considered when defining privacy. For example, a major company director might have serious health issues that will influence his judgment with inconceivable consequences. Making that fact public liberates him from the burden of responsibility and prevents further misfortune. Another example might be a father that files a police report that his daughter is a prostitute.

Therefore, living in civil society obliges us to make public unreasonable personal beliefs that fail public justification, which by themselves can have different scope and model.

Our autonomy is restricted in areas where our actions harm others. Every day we draw a line and respect other's privacy by having that in mind. Generally speaking, protecting our privacy makes us uncomfortable, afraid, and also smarter too. But what if the other isn't a person but an algorithm that predicts the future and by doing so, limits our autonomy, without us even knowing? Private data gathering is called surveillance, a modern-day phenomenon that threatens privacy.

2.2 Electronic surveillance

In the past 20 years, we could witness the rise of surveillance capitalism. The term was elaborated by Shoshana Zuboff back in 2014 in her essay, ”A Digital Declaration” [11]. There she pointed out the generally accepted institutional fact that we live in a society where the person’s life is a well that algorithms for human behaviour predictions drink from. That fact is imposed by the non-violent declarations of higher purpose, which some are unquestionably true, and masked under various services accessibility, improved commodity of life etc.

It all began after the new age of the fight against terrorism and the 9/11 attacks started. Immense political pressure to terminate such a threat to humanity but also the convenience that it brought to the Big Tech industry resulted in Google increasing revenue by 3,590 per cent in the last four years since 2004 [10]. Those events, we may conclude, justified the gathering of everything useful about an individual to protect the public. When did surveillance become a problem for us, the victims? Our first guess has to be: ”When concluded predictions started to be sold on a large scale.”

Zuboff compares the last 20 years that transformed the ontological, economic, and political structures, to the industrial revolution, and the enslavement it brought, from the beginning of the 20th century. Here she refers to Arendt [7], where she reflects on the magnitude of destruction totalitarianism brought and the 20th century’s thinker’s inability to foresee the dark veil that covered the society. The difference is that totalitarianism operated through the means of violence, and instrumentarian power operates through the means of behavioural modification. The main point may be summarised by her sentence in [10]: ”The ability to evade individual awareness, and therefore individual will, is an essential condition for the efficient exercise of instrumentarian power and its economic objectives.”

After the bravery of Edward Snowden (Permanent Record book from 2019) [1], Julian Assange’s sacrifice (WikiLeaks founder) [2] and contributions of many others, counter-declarations started to emerge, such as GDPR law [3] in Europe, taping over the camera lenses on iPads, ”Do Not Track” legislation etc. In recent years, a positive trend can be seen in the composition of new privacy protection laws, but those counter-declarations might as well ignite mighty corporation’s creativity in finding new surveillance methods.

Although it seemed hopeless to protect our autonomy, our will and future, today it may be a different story. In the picture below, we can see an incidence of the word ’privacy’ on the software developer’s main knowledge exchange site.

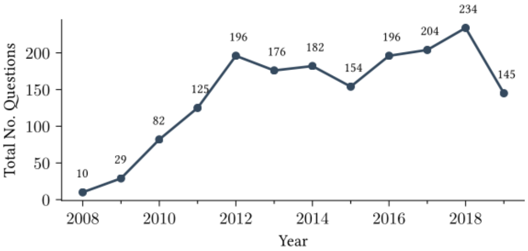

Figure 1: Count of questions mentioning privacy per year.

Source: Understanding Privacy-Related Questions on Stack Overflow [12]

Zuboff urgently calls for a wise way to bypass the direct fight against Big Tech. Based on existing laws, some kind of synthetic declaration may become an alternative institutional fact. That is the digital world where we don’t have to fear the potential fascist entrepreneurs or a panopticon [6]. She points out that either we close the tap or make sure that instrumetarian power is diminished by imposing a stronger law.

[1] Wiki: https://en.wikipedia.org/wiki/Edward_Snowden

[2] Wiki: https://hr.wikipedia.org/wiki/Julian_Assange

[3] Website: https://gdpr-info.eu/

The problem with us closing the tap is acknowledging the defeat and going off the grid or self-censor ourselves. Counter-declaration like self-censorship has an obvious drawback, and that is living in fear. A study from 2013 by PEN America showed that 82 per cent of surveyed writers mind their words because they knew the UK government is collecting data about their internet activity, the rest just didn't use social media at all or avoided googling phrases regarding Islamic fundamentalism [14]. In the next chapter, a description of current, applied efforts to protect privacy, is presented.

3 Implementation of privacy policy

Software development teams can decide which libraries, tools, and platforms to use, what data to collect, and how to present information to users, which means that their choices directly impact user privacy. The next chapter summarises a recent collection of papers 'Privacy by Designers' by Mohammad Tahaei [12].

3.1 Outline of current practise

Developers are the front line between public and private and they struggle with materializing privacy in code. They are guided by Fair Information Practice Principles (FIPPs), a privacy policy framework. FIPP basically requires that :

- User are notified and give consent
- Collected data amount is minimal and has a clear purpose
- Data is confidential and secure
- User can access the data and rectify it

Tahaei presented a survey where it was concluded that developers are confusing privacy with security and mostly acknowledge organizational climate as a decisive force affecting their behaviour when it comes to privacy issues.

The most profound result is that developers are rarely aware when they jeopardize someone's privacy and, in most cases surveyed, don't consider themselves responsible for it.

Very often, developers use advertising libraries that require user sensitive permissions, which sometimes have implemented tools for dark patterns - instances where knowledge of human behaviour and the desires of users, serve for deceptive functionalities. Those libraries are easy to use, but the developer is liable for privacy breaches if it comes to it.

Moreover, platforms such as Apple, Google and Facebook are forging the defining privacy requirements for developers by specifying what 'sensitive' information is and what types of information developers need to communicate to users. Information about new updates are mainly looked up on Stack Overflow [4] website.

Finally, the developer's common practice to protect privacy is to implement basic privacy-by-policy methods that include user control, access, and limitations on data collection or privacy-by-architecture methods such as cryptography, k-anonymity, and differential privacy [1].

3.2 Privacy by Design and Privacy Champions

Privacy by Design is a privacy protection framework that has a bottom-up methodology other methods lack. Those frameworks are privacy-by-architecture, privacy-by-policy and the basic fea-

[4] Website: https://stackoverflow.com/

ture of notice and choice. Ann Cavoukian [5], who coined the term, describes Privacy by Design as: "...assures an end-to-end chain of custody and responsibility right from the very start."

Implementing such a policy requires thorough planning and perhaps disintegrating privacy into smaller understandable elements such as secondary use, exclusion, and breach of confidentiality [12].

Privacy Champion is a title given to usually senior developers with higher moral and ethical standards. To promote privacy, privacy champions regularly use informal discussions, management support, communication among stakeholders etc. Documentation and guidelines for the rest of their team or the whole organization is often used, to promote ethical behaviour [2].

Privacy Champions use or build tools and libraries to assist others in developing privacy-preserving products, testing, and vulnerability discovery. Today's trend is to automate the process in order to prevent third parties to exploit the vulnerabilities.

Moreover, in another survey among privacy champions conducted in [12], the author implies that privacy is hard to measure and lacks standardised definitions and taxonomies. Metrics for evaluating privacy risk and effectiveness of privacy protection approaches are sparse or nonexistent. Apart from fixing above mentioned problems, the author suggests including privacy courses in computer science curricula.

4 Conclusion

The work of modern philosophers and ethics scholars is being heard more often and louder. Organizational privacy climate is defining factor in forming a developer's approach to privacy, therefore more effort has to be made towards reducing their responsibility load, and also investing in education within teams.

Potentially democratic Internet may not be a utopia, but a web of knowledge and technologies and a properly controlled network of people and companies, backed by the enforceable law.

The synthetic declaration necessary for that transition has to be nurtured by the media which promotes companies that are already making the effort in Privacy by Design frameworks.

Soon, we will go to work by wearing the brain-computer interfaces for Extended Reality, while similar gadgets will make us sense the digital world livelier. Therefore, a question could be asked if it can get worse. Well, Slavoj Žižek elaborated in his book that it can [15]. Brain to brain communication and sharing our consciousnesses (vision, emotions, sensations etc.), without time lag, sounds frightening, but that kind of singularity isn't within technology's reach, yet.

It's worth focusing on the Extended Reality Safety Initiative[6], because the data we will probably care about the most could be protected by that body. It seems impossible to resist monitoring our every emotion and thoughts, via the VR set accurately, to use them in the closed code computer game[7]. Though we mustn't forget, western medicine can only flourish with precise drugs, predicting disease prevention methods and effective mental health protection enabled by the emotional feedback provided by such apparatus.

To illustrate, inference by analysis of gathered information is a natural behaviour of any being. As soon as we start to predict the future we lay grounds for premeditation, therefore potential evil. Cheetah intercepts a gazelle, fictional detective Holmes correctly guesses the wanted criminal's gender by examining their handwriting [8] and algorithm skims through sparse matrices containing our previous website visits [4] then connects our profile with a salesman, the predator.

If we are not already at the end of the Gartner's hype cycle [13] of that new technology that sneaked under our skin and attempted to take our future and if it's really not worth the effort then

[5] Wiki: https://en.wikipedia.org/wiki/Ann_Cavoukian

[6] Official website https://xrsi.org/

[7] Analogy to Ready Player One movie, https://www.imdb.com/title/tt1677720/?ref_=fn_al_tt_1

we might stop worrying and start to love their digital world envisioned by the big corporation [8].

[8] Idea was taken from the Dr Strangelove movie, https://www.imdb.com/title/tt0057012/

Bibliography

[1] Irit Hadar et al. ‘Privacy by designers: software developer’s privacy mindset’. In: *Springer Science+Business Media* (2017). doi: https://doi.org/10.1007/s10664-017-9517-1.

[2] Jessica Sierra Beena Ammanath Catherine Bannister. *White paper: Ethical technology in the workforce.* url: https://www2.deloitte.com/us/en/pages/technology/articles/prioritizing-ethical-tech-workforce.html (visited on 15th Apr. 2022).

[3] Fred H. Cate. *Privacy in Electronic Communications, before the Subcommittee on Courts and Intellectual Property, Committee on the Judiciary, U.S. House of Representatives.* url: https://irp.fas.org/congress/1998_hr/h980326cf.htm (visited on 29th Mar. 2022).

[4] Prabhakar Raghavan Christopher D. Manning and Hinrich Schütze. *Introduction to Information Retrieval, chapter 19.* Cambridge University Press, 2008. isbn: 0521865719.

[5] Mokrosinska Dorota. ‘Privacy and autonomy’. In: *Law and Philosophy* 37 (2018), pp. 117–143. doi: https://doi.org/10.1007/s10982-017-9307-3. url: https://link.springer.com/content/pdf/10.1007/s10982-017-9307-3.pdf (visited on 29th Mar. 2022).

[6] Timan T. Galič M. and Koops BJ. Bentham. ‘An Overview of Surveillance Theories from the Panopticon to Participation’. In: *Philosophy and Technology* 30.1 (2017), pp. 9–37. doi: https://doi.org/10.1007/s13347-016-0219-1.

[7] Arendt Hannah. *Origins of Totalitarianism.* Schocken Books, 2004. isbn: 9780805242256.

[8] O’Brien James. ‘Six methods of detection in Sherlock Holmes’. In: *Oxford University Press’s, Academic Insights for the Thinking World* (Sept. 2013). url: https://blog.oup.com/2013/09/six-methods-forensic-detection-sherlock-holmes/ (visited on 20th Mar. 2022).

[9] Richard A. Posner. ‘The Right of Privacy’. In: *Georgia Law Review* 393 (1977). url: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2803&context=journal_articles (visited on 29th Mar. 2022).

[10] Zuboff Shoshana. ‘“We Make Them Dance”: Surveillance Capitalism, the Rise of Instrumentarian Power, and the Threat to Human Rights’. In: *Human Rights in the Age of Platforms* (2019).

[11] Zuboff Shoshana. ‘A Digital Declaration’. In: *Frankfurter Allgemeine Zeitung* (2014). url: https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshan-zuboff-on-big-data-as-surveillance-capitalism-13152525.html (visited on 20th Mar. 2022).

[12] Mohammad Tahaei. ‘The Developer Factor in Software Privacy, collection of papers’. PhD thesis. School of Informatics, University of Edinburgh, 2021.

[13] Wikipedia. *Gartner hype cycle.* url: https://en.wikipedia.org/wiki/Gartner_hype_cycle (visited on 20th Mar. 2022).

[14] Nik Williams. *Writers silenced by surveillance: self-censorship in the age of big data.* url: https://www.opendemocracy.net/en/opendemocracyuk/writers-silenced-by-surveillance-self-censorship-in-age-of-big-data/ (visited on 13th Apr. 2022).

[15] Slavoj Žižek. *Hegel in a wired brain.* Bloomsbury Publishing, 2020. isbn: 9781350124417.