From personal security to surveillance capitalism

Author: Domen Savič

Version: 1.5

Table of Contents

1. Introduction into the surveillance capitalism and course outline

How will you benefit from this course, what problems we are addressing and why is this course different from the others.

Data economy turned us into products. Our daily lives, our activities, our thoughts are mapped out, collected, analyzed and then sold to the highest bidder online. Social media networks, mobile apps, services and gadgets are tentacles of surveillance capitalism, rigged against us and our privacy.

We can fight surveillance capitalism on three different levels. We can fight it as citizens, we can fight is as consumers and in your particular case, we can fight them as journalists. We will our time together to analyze the current situation, offer practical privacy-orientated solutions but also invest into the media agenda setting that needs to take the practices of surveillance capitalism seriously.

The reason why we are banding together different aspects of surveillance capitalism is simple - you cannot fight it alone. You cannot fight it just from from a position of a consumer. You cannot fight it just from a position of a citizen. There needs to be a systemic approach to addressing these issues and this training will hopefully offer examples, principles and concrete habits that will help you do that.

The first day will focus on personal digital security. We've set 6 topics aside, covering everything from data security to biometric surveillance protection, mobile devices and work in the field to office work and personal computer protection. We will debunk some of the prevailing privacy myths that actually hurt people that seek to protect its privacy, offer workable solutions that secure your privacy and help you out protecting and securing your data and communication channels and offer other examples of privacy-orientated behavior.

When we talk about surveillance and invasion of privacy, we usually think about the good ole days of state surveillance agencies that employ spies that target individuals based on their characteristics. Journalists, activists, opposition politicians... these people are usually the prime targets based on their beliefs, social power or the ability to move large groups of people. The idea of people spying on people is engraved in literature, pop culture and other venues of our social lives. When asked about the importance of privacy, people usually reply: "I have nothing to hide".

The response is completely normal and completely irrational at the same time. It tells us more about the perception of surveillance capitalism than of the actual threats that are present in the digital environment of communication tools and services that we use every day. At the same time it explains how big actors in surveillance capitalism are getting away with their practices.

Another aspect of surveillance capitalism that we need to take into the account is its omnipresence. It is literally everywhere and with the expansion of digitization in the areas of smart city and other public spaces, our home appliances and cars and other venues of public lives it will only get worse. This omnipresence is a direct source of another concept that you should be aware of – privacy fatigue.

Privacy fatigue happens exactly because of the sensory overload of too many threats that await us. You have to take care of your devices, of your services, you have to watch out for the mass surveillance practices offline and online, you have to... at one point the person says: "You know what – I don't care. It will never end and it's pointless to resist." This again is normal. After all, almost every policy in this field puts the burden of security on the shoulders of an individual. GDPR, cookie directive, account access approvals... everything is hinging on your attention and your focus in order to do the right thing.

Failure to do so is attributed to many different factors. Can you think of any? Why do you think we suck at protecting our own privacy? We could separate the reasons into different category.

One is definitely usability and speed. Privacy is slow. Privacy is not useful. If you want to securely log into your phone using the best possible security practices, this will take longer than just by logging in via biometric solution. If you want to securely talk to a colleague, the correct way to do so will limit your abilities to share documents, if you want to securely exchange data this will again be extremely cumbersome and slow. And since journalistic work needs to be fast, the security usually takes the back seat.

Second is the previously mentioned overload. It's just too much stuff. It's social media channels, it's phones, it's tablets, it's computers. It's the way we pay for things, it's the way we move through space, it's the way we interact with each other. A human being is a social being and privacy is extremely anti-social.

Third is the social aspect of surveillance. Even if you try or actually do everything right, there's a big chance that somebody else will rat on you. Surveillance, focused or general, is extremely good at using the social aspects of our society against us and this makes everybody vulnerable, even if we are trying to be good.

Fourth is the political aspect. Surveillance is political. It usually follows an obscure path that connects the industry and decision makers and needs to be taken and investigated as such. Focusing solely on personal responsibility makes less and less sense because the real power lies in the decision-making process that legitimizes surveillance society and offers little to none resistance after the fact.

I am slowly wrapping up. We're going to take a short break before jumping onto our first exercise of the day – privacy-orientated practices of using a personal computer. We'll try to cover as many different aspects of it, but feel free to ask questions about a particular subject and I'll try to answer them.

2. Personal security: Personal computer

How do you harden your personal computer, what are some of the biggest privacy/security mistakes you can do and how to avoid them.

These tools are one of the biggest thieves of our personal and other data because of several reasons.

First reason is obvious – we do everything with them. We combine private and public sides of our persona on them, we use them for our work and pleasure. All of the data points we produce can and actually are used to surveil our activities. Second reason is the dangers connected with the previously mentioned sensory overload. Clicking on a link, opening an email or any other user activity can trigger the malware that executes data theft. Third reason is poor security culture that usually does not plan for regular backups, anti-virus solutions or other preventive measures that protect and prevent some of the attacks.

2.1. Forms of attacks against your personal computer

Let's take a look at some of the ways personal computers can be a privacy threat so that we can then develop an effective ways to counter those threats.

a) Physical data theft

One of the simplest ways is the good old data theft via classic act of thievery. Computers are getting smaller and smaller and it's easy to put them in a bag or a backpack and run away with them, leaving the previous owner without it.

b) Physical access to the system

Similar to physical data theft is the physical access to the system where the attacker gains physical access to your computer via break-in or similar procedure. This usually happens via password hacking or gaining access to a computer that is not protected by a password.

c) Remote access to the system

Another popular way of privacy invasion is remote access to the system via web-based service or a specific software. The threat usually involves the owner clicking on a dangerous link that triggers the connection.

d) Ransomware

Hijacking your computer and then force you to pay the hijacker is becoming more and more popular due to the expansion of cryptocurrencies that hinder anybody who wants to follow the money.

2.2. How to secure your computer

a) Regular backups

It sounds corny and boring, but backuping works. Ransomware is an ever-growing threat and regular backups plus a system of data storing can help in a big way. What and how to backup depends on your particular situation, it's useful to invest either in cloud storage or local detachable disk sets.

b) Anti-virus solution

They work. Not all the time and not always 100%, but generally speaking you're better off at having an anti-virus solution installed on your computer than you are without one. They might slow down your computer or other device, but at the same time they offload a great deal of attention you'd otherwise spent on figuring out what to click and what not to click.

c) Good passphrases

This is not a typo, you should think about replacing passwords with passphrases, the main difference being that passphrases are based on sentences which automatically prolongs them while at the same time secures its complexity. You can even invest in password managers which will help you generate specific passwords for individual accounts – recycling passwords is one of the most common mistakes users do because of the overload of user accounts.

d) Separate accounts

If you are using the same computer for business and private affairs, you need to think about separating user accounts and keep as much files and logins separate from one another. The best solution would be to use two devices but that is not always a possibility.

3. Personal security: Mobile devices

How to harden your mobile devices, which threats are most common and how do you protect yourself from them.

Smart phones are becoming more and more important in our digital lives, since their processing power and cloud-based apps and programs are replacing desktop computers and laptops.

3.1. Forms of phone-based surveillance

Let's take a look at some of the ways smart phones gather our personal data, resell it to other parties and threaten our privacy.

a) App-based surveillance

A huge part of app economy is based on surveillance advertising model where apps track your digital habits and sell that knowledge to different advertising companies. This enable the companies to target you with relevant ads and at the same time make a very detailed profiled of your online habits that can be used against you. Also dangerous are apps from unofficial sources that offer new possibilities but are in fact just disguised ways of targeted surveillance and malware.

b) Phone OS-based surveillance (zero days threats)

Software and hardware has holes. Holes are dangerous. Zero day threats mean that they are unknown to the phone manufacturer which makes defending against them harder. Generally speaking you're better off buying a respectable phone brand and updating your phone software regularly.

c) Targeted surveillance (spyware, malware)

Spyware and malware solutions are becoming harder and harder to detect, once you are targeted. Generally speaking they still have to include a specific message with a link the user has to click on or at least open, even though this is not always the case. Generally speaking, a good anti-virus solution and caution when opening messages from unknown sources should somewhat deter targeted surveillance.

d) Different type of signal surveillance (IMSI catchers, bluetooth)

Mobile phones signals (GSM, bluetooth) can be used to latch on to surveillance systems like IMSI catchers or bluetooth signal hijackers. The only way to prevent these types of attacks is with a Faraday cage.

e) Physical loss of phone

Losing your phone is a nightmare. There are some things you can do to limit the damage.

3.2. How to secure your phone

Although imperfect, there are some ways you can harden your smart phone against different attacks. Generally speaking these advice will help you out defending against specific attacks, but are not bullet-proof.

a) Limit apps and update your phone regularly

Simple advice and easy to follow. Be mindful of your phone usage and update it with official updates only.

b) Set a strong passphrase and don't use biometric locks

Locking your phone and a strong passphrase while ignoring the biometric techniques of unlocking helps securing your phone and data on it in case of theft. You can turn on the wipe data function while using an iOS operating system to further secure your data and prevent dictionary attack.

c) Use privacy-orientated apps

Privacy-based economy is booming due to the recent scandals in the field of information technology. Apps and services that value user privacy and offering reasonable payable subscription options represent an alternative usage. Also worth considering are open-source apps that value privacy and are usually free.

d) Use Faraday cage

To prevent IMSI and other signal-related attacks, we are providing each of you with your very own Faraday cage. Stick your phone in one and you are good to go. Be careful – the cage does not limit recording of sound, so if your phone is infected with a spyware that records sound, it is best to keep it away from the source of sound you want to keep private.

e) Safely backup your phone

Similar to the advice with your computer, think about backing up valuable data on your phone so that you always have a copy of the most important documents and contacts off-phone.

4. Personal security: Online services

How do online services get our data, how to we avoid leaving too wide of a digital trail online and how do we reclaim our data from the web?

We are continuously exporting our life online. Almost literally, as we use social media accounts, web services accounts and other online-based features to conduct business, lead our private lives or keep in touch with our sources and professional colleagues. At the same time, app-based economy and surveillance advertising model are threatening our privacy on every step of the way.

4.1. Forms of online services surveillance

Here are some of the general ways of surveillance that comes into play when we use online services and features. These types of surveillance are a combination of several factors that include technological capabilities, workflows of interest groups (criminals, governments, other entities) and

a) Service-based surveillance

The most common surveillance in today's digital economy. Free online services usually involve data gathering and analysis that can then be sold to the highest bidder on different ad and private data marketplaces. Usually this type of surveillance is not user specific, but is focused on large groups of users, although it can also be used to target specific user in many ways.

b) Ad-based surveillance

Ad-based surveillance is the latest systemic tracking of users online through ad-services that monitor our behavior online via computers and smart phones and then report our habits back to the owner of the monitoring system.

c) Internet traffic surveillance

This is an enhanced way of surveillance that usually involves spyware or the involvement of a telecom company. Surveillance is done on a device which monitors the target's traffic and then picks out the relevant parts. It's extremely dangerous as it can include ALL of the data streams the use is transmitting.

d) IoT-based surveillance

Another way of online service surveillance is via IoT devices that are becoming more and more popular. Smart TVs and other devices in our homes of places of work gather and transmit data and monitor our data behavior, stripping us of privacy.

e) Smart city surveillance

Not really an online type of surveillance, but fits the profile as our cities get more and more connected and equipped with monitoring solutions from smart trash cans to surveillance systems that follow us in public spaces and monitor our public behavior.

f) Biometric surveillance

Even though biometric surveillance is usually tied to offline activities, there is still a threat of biometric surveillance online as the web represents one of the richest sources of material that can be included in the biometric databases.

4.2. How to secure your online services

Here are some practical solutions that can help you secure your online identities and help you navigate the online environment. They will not completely anonymize your behavior, but they will limit the size of your digital footprint which might hamper attempts of surveillance.

a) Use 2FA-based logins

If you have not already, you need to turn on 2FA on every possible online account you own and use hardware keys combined with mobile apps for authentication. We've supplied every attendee of this training with a Yubikey hardware solution and we're going to show you how to use it.

b) Use privacy-orientated services

Try and change up your digital habits, replacing your usual services with ones that are more privacy-orientated. Find more information at https://privacyheroes.io/

c) Use privacy-orientated tools

Try and change up your digital habits, replacing your usual tools with ones that are more privacy-orientated. Find more information at https://www.pcmag.com/picks/essential-apps-for-protecting-your-privacy-online

d) Use zero-knowledge storage

Another important tool is zero-knowledge online storage. Zero-knowledge means that nobody can access your data without the password and username and there is no way for the provider to access your data via administrative access.

5. Personal security: Biometric surveillance

How does biometric surveillance works, why is it so hard to avoid and what are some common misconceptions about it?

Biometric surveillance is becoming more and more prevalent, as it is usually combined with the smart city solutions and surveillance technology that is used to access-control in work places and other venues.

Police through-out the world are relying on biometric databases to hunt for criminals and control the masses, the advertising industry is using biometric information to target users with specific ads and there is an ever-growing threat from the private sector that uses biometric data for variety of reasons.

5.1. Forms of biometric surveillance

Let's take a look at some of the forms of biometric surveillance and places where they are used.

a) Finger prints

Most common and widely spread biometric surveillance practice that is used in everything from access control, identity confirmation, basic surveillance... It's cheap, it's perfected and since there are many toolkits available, almost everybody can use it.

b) Facial recognition

The second most obvious and most used biometric surveillance method is using your face features to track your movement and identify you in the photos. First user case are our smartphones and computers that use facial recognition for user access. Second user case are social media apps and other online services that use them for customer identification. Third is police and security surveillance, fourth is advertising. First most common user case is border control.

c) Palm prints

Palm prints are similar to finger prints, but they use more details and are usually more precise, although systems for palm prints detection are more demanding. Palm prints are privacy-orientated, as they cannot be obtained randomly and do not tell anything about the owner.

e) Other types

Body odors, gait analysis, retina scans, keystrokes, heartbeat, voice, veins, ears, DNA... are some of the more special types of biometric data that can be analyzed and stored. They are usually more technologically demanding and not used in general population yet.

5.2. How to avoid biometric surveillance

Wear a paper bag on your head at all times. Which is a very impractical solution. Commercially available systems for biometric surveillance are becoming more and more advanced, as you can see in the experiment we did with Amazon Rekognition system. The only solution is effective legislative framework and workable execution that prevents these systems from being present in our society.

“One of the issues with these biometric surveillance systems is the idea that we can tackle any social problem by using the right technological solution,” ponders junior research fellow at the Institute of Criminology at the Faculty of Law Ljubljana, Pika Šarf, who asks the question: “Can facial recognition really achieve a certain goal in terms of improved security and policing, and if we can, is this solution really the least invasive measure that can achieve the same aim?” and highlight the lack of reports on the successes of biometric surveillance systems. “If we examine the large centralized data bases which are used to monitor travel flows in and out of EU, we can note that the EU rarely provides the data on how many times were these systems able to intercept a “problematic individual” from crossing the border and how many criminal cases did they thwart with it,” she notes.

“It all comes down to data set and their quality,” explains assistant dr. Žiga Emeršič from the Faculy of Computer and Information Science at the University of Ljubljana.

He is mainly focusing his attention at biometry, deep neural networks and computer vision. “For a working facial recognition system, you have to pay attention that the data includes obscured faces, photos of faces in low resolution, different angles of shots… all of this matters when you are training a facial recognition algorithm,” he says.

His faculty colleague, assistant Blaž Meden who is focusing on the field of facial recognition models anonymization, explains further. “Models of neural networks that are used in facial recognition systems are constantly changing. In my work where I try to “break” the faces in a way that they’re still recognizable by humans but not by machines, I find it increasingly difficult to do that successfully,” says Blaž Meden, “since the facial recognition technology is getting better and better.”

Biometric surveillance is becoming more and more prevalent and commercialized. At the same time there’s very little if anything that can be done from the point of the user, as we have shown. Technology is a political issue that needs to be addressed as such. Unless of course we are comfortable with the world where the only thing protecting your biometric privacy is a paper bag over your head. Or for the time being – a Batman mask.

6. Personal security: Threat scenarios

Role-playing of different threat scenarios that include before-mentioned technologies and strategies of privacy-enhanced behavior.

To develop an effective and workable defense, you first need to answer these four questions:

- What do you want to keep private?
- Who wants to know?
- What can they do to find out?
- What happens if they succeed?

Answering these questions involves building up a picture of the security problems you face: a threat model. Building a realistic model requires that you understand both your adversary and the relevant technology. You will need to research what your adversary and similar adversaries have done in the past, to build up a model of what they want and what they might do.

You will need to look under the hood of the technologies you intend to use, and understand how the technical intersects with the legal, physical, and social. After that—when you understand the security landscape you are operating in—you can move on to defining specific processes and tools to meet your needs. But plans and tools don't make security; clear understandings and diligent habits do. The simplest plan you can come up with might be the best.

We're going to split into five groups. Each of the group will get a challenge and will present its best solution for the issue to the group.

6.1. Threat scenarios

Here are the scenarios. You will now split into groups and work on individual scenarios. You'll study the challenge presented to you and devise the most useful, applicable and complete security solution, which you will then present to the class.

a) Threat scenario 1: Securely talking to a source

You are writing a story and a previously unknown source reaches our to you via work email address with a scoop. What are some of the threats you need to watch out for and how do you securely establish a line of communication that does not threaten your source and at the same time enables you to verify its information?

b) Threat scenario 2: Working in a secure environment

You are producing your work in an office and use an office computer that is separate from your personal computer. How to you secure your work documents and files if you want to protect them from random burglary or targeted investigation?

c) Threat scenario 3: Securing your online services

You are in charge of taking care of publishing the work of your colleagues online. How can you secure your online services that help you out in this regard?

d) Threat scenario 4: Covering live events

You are covering a live demonstration of a government's opposition parties. There's a large group of people gathered, the police is present as well. How do you protect yourself and perform your duties as a journalist?

e) Threat scenario 5: High-priority target A

Because of your work, you are a high-priority target for your government. How do you cover your tracks and secure your work and communications?

f) Threat scenario 6: High priority target B

You are finalizing important investigation which could bring big public outcry. Suddenly you realize that you are followed on the streets by unknown people and you suspect also your home and office are under surveillance.

7. Politics of surveillance capitalism

What is surveillance capitalism, how does politics worsen the situation and how can the media reporting improve it.

To address surveillance capitalism is to start rethinking the role of tech journalism. Technology sector is where the surveillance capitalism was born and we need to start thinking about the way journalists usually cover news from Silicon Valley or other places of techno-Meccas.

First question we need to address is who are our sources when we are addressing topics that revolve around technology. Usually we tend to form our own "quote circles" where we recycle same academics, same private sector representatives, same public speakers on certain topics. This creates a "filter bubble" where certain ideas from specific sectors adopt a shape of "common knowledge" and some never see the light of day.

Second question revolves around the issue we're reporting. Tech companies are more and more embedded with foreign policy goals (China and US are the same in this regard!) and covering a tech issue without noting these connections might skew the perception of the reader. Think about Huawei and Belgrade or Brussels lobbying efforts of Western Big Tech industry - these issues are rooted in politics and spheres of influences, not technology.

Another issue that we will address moving forward is the relationship between media outlets and tech companies. We have seen different ways tech companies are trying to curry favors with media outlets, offering them exclusive materials, buying ad space and using different tactics to influence their reporting on them.

Third thing we need to take into the account when covering the topic of surveillance capitalism and the role of big tech companies with political backing is what is the scope of interest with our target audiences and how else is involved in the process.

Fourth, we need to re-examine the role of the user. Currently the tech industry and decision-makers are unified in the theory that the user should be responsible for everything. GDPR and other legal frameworks hinge on an active user and almost completely neglect the dysfunctioning aspect of regulators, limited reach of local DPAs and lack of user knowledge and skills needed to tackle these issues.

The media outlets with their current pro-tech reporting that treat the entire field as a consumer issue instead of addressing civic concerns are deepening the problem. As they consumers think they are left to their own devices and skills, there is little to none expectation of anybody else to address the issue

from a regulatory or legal perceptive. This creates a unique death-loop where the industry is manufacturing privacy-invasive solutions and practices that are then passed onto the "active user" who is responsible for limiting their damage.

8. Surveillance capitalism media discourse

What's wrong with today's surveillance capitalism media discourse and how can we make it right?

Let us think about the last three journalistic pieces that come to mind when I say surveillance capitalism or big tech. What are they? We can quickly see that journalism is constantly resorting to "shock doctrine" reporting when it comes to issues of big tech without addressing the systemic corruption practices and other issues that exists in this field.

Media discourse of surveillance capitalism fails to address political and social issues connected to this field. Can you think of some reasons for this failure?

8.1. Reasons for failures

Let discuss the issues that hamper tech journalism today and fail to represent the issue of surveillance capitalism in the useful light.

a) Journalists are failing at seeing the big picture
Usually, reports in the region from the field of surveillance capitalism fail to see the role of the private sector and instead focus almost exclusively on the role of the state. As you move further to the West, the role is reversed – the state is almost never mentioned in the reports, at the same time everything revolves around companies.

b) Physical component of surveillance capitalism
Especially, but not exclusively, TV reporting focuses on visually-attractive reporting about concepts and in the case of surveillance capitalism. This hampers the concept of opaque surveillance practices and other concepts that are not represented easily.

c) The fake neutral role of technology
Another issue is the supposed neutral role of technology. Algorithms, big data sets and other technological achievements are usually represented as neutral, without biases. Even when reporting on clearly biased decisions, the reporting forgets to approach to the issue more broadly.

d) Car is a horseless carriage
When journalists are trying to explain new concepts, they sometimes use outdated metaphors that do not reflect the current situation as people usually think: "OK, so if this problem is like that old problem, then surely we already have a solution in place." We do not.

e) A victimless crime
Reporting on privacy invasions usually fails when the journalist cannot find a victim that would fit the crime. Since there is no "body", media reports usually fall short at bringing the reader's attention to the severity of the issue.

f) Long tail of (boring) responsibility
Reporting on hacks, attacks and other cyber-crimes might be interesting, but to investigate the chain of responsibility usually takes too much time and energy and does not guarantee the results will be flashy enough.

8.2. How do we improve reporting?

a) Take a step back
Seeing the big picture that includes private-public partnerships, geo-politics and international relationships will make you see the problems better and offer you a wider field of analysis.

b) Intersect human rights, business and politics angles
When focusing on a tech issue, you need to include human rights, business and political angles when addressing it. This will help you in expanding the roster of potential speakers, at the same time it will enable you to address the issue from another perspective.

c) Define your audience
Taking a deep-dive into different roles of your audience in relationship with the topics of surveillance economy. Do not define them just as consumers, but focus on different roles like gender, ethnic background and other human rights sub-groups.

d) Inspect your role in shaping the discourse
You need to be aware of your role as a journalist when it comes to shaping the discourse. Since the field is still developing with many actors trying to push their own narrative as the prevailing one, the journalists are the ones who can amplify or silence individual voices.

9. Supply chain of surveillance capitalism

How do you investigate surveillance capitalism, what are some of the common stops from the factory to the place where you live and who gets involved in the process?

Surveillance capitalism is based on trading with data. This turns every tech company into salesman of data-points that are included into products and services. "Patient zero" is therefor the social contract that depicts the surveillance capitalism business model as the way of the future and everything else stems from this root.

9.1. Supply chain links

a) Tech industry
Tech industry is based on a promise that the companies are good at gathering and selling data points to the highest bidder. This in turn fuels the data-collecting economy of apps, free services and other products that have only one goal - sucking up as much data as possible.

Tactics: Painting themselves as saviors of social problems and skirting away from any responsibility when solutions do not solve anything, but make things worse.

b) Advertising and PR industry
Their role is to package and reform the products in services in accordance with consumer trends and provide talking points for the journalists. This is usually done by invoking lifestyle focus points that obscure the fact that products and services are basically data funnels.

Tactics: Offering exclusive access and other benefits to press for non-critical reporting.

c) Whistle-blowers and activists
There's a special group that is becoming more and more relevant in this field, as it provides an "inside" look into the dealings of the industry from different perspective. They also tend to cut through the noise of the advertising and PR industry, although they can be hard to reach out to. We'll talk about this in the next chapter.

Tactics: Using hard to get information (whistle-blowers) and public pressure to shine a light on practices that the companies do not want to disclose. Beware of fake NGOs, associated with the industry of the decision-makers.

d) Media outlets
This is you. You are suppose to filter out the noise, figure out the way to present these topics to your audience and remain independent from all the interest groups pressures. Media is in charge of strengthening the discourse and highlight talking points from all interested parties and then translate them into actionable content for your audiences.

e) Lobbying groups
Another party in the supply chain are lobbying groups from different actors that have almost unmitigated access to decision-makers and use different tactics to spin public opinion in their favor. This presents a problem since they often use NGO and other seemingly independent actors to further their own cause.

Tactics: Working behind the scenes, placing ideas and interpretations in the mouths of other public actors while working for a particular interest group.

f) Decision-makers
Based on your input as a journalist and inputs from other interest groups, the decision-makers ponder and eventually take regulatory measures to stem the tide of surveillance technologies and services.

Tactics: Bending toward the group that is able to establish a prevailing narrative of the issue.

9.2. Countering interest groups tactics

Here are some of the tactics that you can use as a journalist to counter other interest groups in the field. Be aware that publishing industry is one of the interest groups so you might already be partial to the issue from the start.

a) Follow the trends
Analyzing and keeping up to date with the happenings in the field will help you predict and foresee actions of different groups in the field. This will help you filter out the "breaking revelations" and others shock doctrine practices that interest groups use to mask their cause.

b) Set your own agenda
Instead of deciding which agenda to adopt, try and figure our your own agenda to promote through your work. You are allowed to have opinions and if those opinions are backed with good practices of human rights respect, role of the democratically-elected government and working institutions, your report will resonate the general audiences.

c) Cover all the basis
Don't pick out just the most talked-about sides of the issue but try and cover all the basis, bringing to light less discussed sides of the issue. This will enable you to open up public dialogue and get responses from relevant parties that are not in accordance with their agenda. Persistence matters!

d) Follow the red lines of human rights, consumer responsibilities and citizens impact
How will the issue you are reporting on impact human rights, who will guard citizen rights and what is the role of the consumer and citizen.

10. Surveillance capitalism and investigative reporting

Case studies of surveillance capitalism investigative reporting from the region with highlights of particulars.

Let's discuss some of the regional reporting on the topic of surveillance capitalism and highlight issues and sides of the argument. We'll discuss actual stories from the region, noting the journalistic approach and highlights and discuss problems with the framing of a public debate.

10.1. Relevant stories

Let's discuss the following stories, highlighting political, sociological, economical and other aspects and try to formulate an effective reporting strategy.

a) Serbia: Belgrade Huawei Smart City
Chinese company is installing surveillance system in the capitol and at the same time using this project to influence political decision-making in areas related to Chinese interests in the region.

- Who are the actors?
- What's the human right impact?
- How does this impact the consumer and citizen?

b) Slovenia: Industrial agreement signing
Government is signing agreements with champions of US tech industry (Google, Apple, Nvidia...) in the field of education, science and research where companies will "invest" money in Slovenia.

- What is a potential downside of these agreements?
- Who is monitoring the execution of these treaties?
- How does this influence the role of Slovenia in the EU?

c) Croatia: Border control and surveillance technology
Government is installing border surveillance systems that are used to track illegal migrations and help the authorities with their capture.

- Who watches the watchmen?
- What's the source of the technology?
- How effective are these systems?

d) Region: Ransomware attacks
Private companies and local institutions are getting attacked by ransomware, hampering its functionalities.

- What are the national strategies in this regard?
- Who is responsible for the defense management?
- How does this impact the consumer and citizen?

e) Region: Surveillance advertising
The issue of advertising industry that is using surveillance tactics embedded in digital advertising solutions is one of the hottest topics currently discussed in the EU.

- Who are major involved interest groups?
- Why should you care?
- How is media conflicted about this issue?

f) Region: Covid-related surveillance
Pandemic caused an up-tick of different surveillance practices, aimed at curbing the rate of infections. From phone apps to camera monitoring systems and other applicable technologies, privacy experts warn about the normalization of surveillance.

- Management of crisis
- Who tracks the trackers?
- What happens next?

10.2. Issues and set-backs while covering these stories

Let's try and imagine the issues and set-backs you'll encounter when reporting these subjects and then try and prepare an effective counter-strategy.

a) Finding the right voices
How do you find representative voices that will show the complexity of the issue, who can you contact locally and how to reach out to foreign sources?

b) Getting the relevant materials
Where do you think the relevant materials for covering your story could be and how could you get it?

c) Waiting out the clock
One of the beloved tactics of representatives of power is stalling the responses and documents until the public attention shifts or journalists get assign to other stories. How can you prevent this from happening?

11. Surveillance capitalism: Local and global politics trends

How do global politics trends influence the development of surveillance capitalism in smaller countries?

There are several trends that are helping define the wider area of surveillance society and its tentacles. Getting acquainted with them will help you predict actions of specific public and private actors in the global and local environment and help you with your reporting and investigations.

Trend 1: Automated surveillance
First trend focuses on capabilities of automated surveillance techniques that is based on algorithmic prediction engines and cutting out the human factor. These topics include bias algorithmic solutions, inclusion of algorithm monitoring and the privatization of public data as companies are spreading their influence in the fields of health and other public services.

Trend 2: Corona-related surveillance
Corona pandemic is one of the key reasons for new implementations of surveillance solutions that claim to be "temporary", while in fact the pandemic is being used to normalize "always-on" surveillance techniques and solutions that will remain in place even after the pandemic is not an issue anymore.

Trend 3: Malware and spyware
Spyware and malware, state actors and business model of spyware industry is becoming more and more relevant as cyberwarfare and other usage scenarios are becoming more and more prevalent. Aspects to consider – state's role, impact on local industry and individual, business cases.

Trend 4: Growing regulatory frameworks
EU and USA are gearing up to beef up regulatory models of different aspects of surveillance industry, from advertising to military usage. EU is positioning itself as a "human rights leader" that will have impact on citizens, consumers and digital users across the globe.

Trend 5: Militarization of police forces
The use of military technology in the field of surveillance, spanning from drones do complex information systems is becoming more and more prevalent in the local police sectors as well. Databases, algorithmic surveillance and other tools of surveillance capitalism are getting funded with public money and at the same time create a new battlefield in local environments.

12. Activism against surveillance capitalism

What are some meaningful anti-surveillance capitalism campaigns in the region, what can we learn from them and how can we use activism to effectively fight surveillance capitalism?

Digital activism has developed in the recent years with the up-rise of topics, related to the human rights in the digital sphere. At the same time, we have all seen the lacking of online tools that were heralded as silver bullets in the past. Digital activism now walks a very thin line between interests of the local and global industry, local and global politics and complex socioeconomic relationships.

Here are some of tips and tricks of effective digital activism approach and some of the issues that digital activists face during their work.

12.1. Building blocks

How to start building digital rights activism stance and what are some of the building blocks that will enable you to play this role sustainably and effectively.

a) Know yourself
Define your goals and focuses before the beginning of work or campaign. Address your focuses and fields of attention. Also important is to start thinking about ways of sustainable funding opportunities that will not depend solely on one source of income.

b) Define your target audiences
Think about the people who will care about your stories. Who are they, what do they do and how do they interact with each other?

c) Do a market research
Map out already established activists that address similar issues and note their approach and their short-comings. Also map out relevant institutions in "your" field, so you will know how your protagonists and antagonists are.

d) Develop a communication strategy
NGOs main tool and weapon is an effective communication strategy that enables you to push your messages towards the relevant audiences and make them react in a predictive way. The strategy should include previously defined goals and audience characteristics and the way your messages will reach them.

e) Plan regular activities
These can be meetups, investigations, article publications, calls to action... The important thing is to plan them out so that you have a sustainable activity levels that leave a permanent mark. When planning activities, be mindful of the media relations as well, so that your activities are represented in a broader perspective.

12.2. Relevant targets of digital activism

You probably already know which topics you want to address and what organizations are relevant in this field, but it does not hurt to review some of the most obvious ones and discuss the ways to engage them in a meaningful manner.

a) The state
The state is usually involved in all of the things that go on in any field. They are usually the instigators of new practices via framework propositions or they are working on developing a regulatory framework that monitors certain fields.

Best practices: Testing out regulatory model in practice, tracking public spending and investigating lobbying meetings.

b) Big domestic companies
Big domestic companies are usually involved in public tenders, can easily sway public opinion and influence media reporting via advertising contracts.

Best practices: Analysis of advertising campaigns, data-dumps, practice investigations

c) Big foreign companies
Big foreign companies are usually involved in decision-making processes via lobbying efforts and other practices. You can also compare notes of their activities abroad and locally and question the differences.

Best practices: Analysis of lobbying efforts and meetings, calls to reaction on a local market, forcing them to state their position publicly...

d) Adoption of legislative proposal
Before the law gets written and voted on by democratic institutions, an NGO can influence the public opinion and provide talking points that need to be included in the final draft of the proposal.

Best practices: Engaging in a decision-making process by letting the people know the background and negative consequences and preparing a way to gather and channel public opinion on a specific matter.

e) General public
Awareness-raising campaigns are usually the best way to get people's attention, although you need to me mindful of the address, focus and results of the campaign. Planning ahead usually pays off, as you establish yourself as a relevant representative for a certain topic.

Best practices: Events, discussions, investigations...

Cheat sheet

Here are some quick tips to raise your security level and limit your digital footprint on your phone, computer and internet.

Phone

- Update your phone regularly
- Keep your connectivity possibilities turned off and turn them on just when you need them
- Perform regular checks and remove apps that you do not use
- Use faraday cage
- Use complex passphrases
- Use anti-virus solution

Computer

- Perform regular encrypted backups of your content
- Separate your private and business activities
- Update your software
- Use anti-virus solution

Internet

- Use privacy-orientated tools
- Limit your digital footprint and separate your work and leisure activities
- Use two factor authentication
- Use password manager

Habits

- Minimize your digital footprint
- Separate your work and private flow
- Practice security protocols

Reference links

Database of privacy-orientated tools
https://www.privacytools.io/

You will find privacy-orientated solutions and replacement for almost every possible user case scenario.

Database of privacy and security protocols
https://cpj.org/emergency-response/pre-assignment-preparations/

A list of protocols for almost every risky situation.

List of EU-based privacy NGOs
https://edri.org/about-us/our-network/

You will find a list of NGOs that are working in the field of digital privacy and security through-out EU.

List of privacy/security news sources
https://blog.feedspot.com/cyber_security_news_websites/

One of the helpful lists to follow the happenings in the field of privacy and security.

Risk assesment chart
https://cpj.org/reports/2012/04/assessing-and-responding-to-risk/

Helpful guide to asses risks and mitigate them on the go.

Threat modeling
https://helpdesk.rsf.org/training/your-threat-model/

A helpful tool to asses threat model and develop an effective counter-strategy.

13. Digital Activism

When talking about digital activism, we are first presented by a question of definition. What is digital activism? Different groups see digital activist differently, comparing Anonymous movement to people who teach the usage of digital tools and everything in between.

Can you be a digital activist without using digital tools and can you use digital tools as a consumer but not as citizen? Since the technology is expanding into different venues of our public and private lives we can conclude that digital activism when defined in the broadest of senses, focuses on civil rights within the society of information technology.

Furthermore – is digital activism a civic or a consumer's duty? Should we address the issues of surveillance, freedoms, privacy and other issues that connect to the digital technologies from a point of an individual or from the collective stance?

Finally – what should be our field of operations? Does it matter if we (re)act on a local level or should we focus on the global policy development? Is the role of a digital activist connecting different interest parties and facilitate a debate, should activist represent certain interests and whose interests are those?

This training focuses on examining good practices of digital activism from the region, offers some guidelines on how to start and maintain your activist position and what are some of the topics of human rights in the digital sphere that are currently worth examining and pursuing.

It also offers practical advice on how to develop your policy and communication strategy for your digital activism, based on several years of work in the region. Finally, it addresses the issue of successful media relations that can help you promoting your causes and improve your communication skills when presenting it to the general public. The training aims to improve regional NGO practices and in combination with digital security training offers a complete introspect into the activities of a modern digital NGO.

At the same time, digital activism offers a few very specific pitfalls that can render it ineffective and turns activists into hapless advertising billboards for specific causes. The root of the problem? Financing of the NGO sector and strings that come attached to some of the funds which renders the NGO ineffective in pursuing their goals. This is especially troublesome when examining the field of digital human rights, since this is currently a hot political and economical topic with a huge number of different local and global actors that are trying to push for their agenda and influence other parties, included in the process.

This in turn opens NGOs up to a huge number of risks that are related to their funding sources. Since we can say that almost entire NGO sector in the Balkan region is funded primarily by local and global public funds this creates a very problematic position for the NGOs that try and oppose the policy developments, offer alternative takes on solving issues and test already implemented solutions. Since

money with strings usually does not allow for the focus on recent developments but rather selects the subjects that are further down the pipeline, the NGOs are usually left with picking up the slack, while the hot issues remain unaddressed.

Of course, there is a relatively simple solution – the NGOs liberate themselves from the bonds of public funds and pursue other ways of funding their activities, therefor assuring their independence, flexibility and persistence. This is easier said than done, but it is worth at least considering.

Another issue that is connected with the digital activism and hampers the effect of activists is the so-called "illusion of participation" where the techno-deterministic use of digital tools dictates the meaning of messages and limits their reach to online filter bubbles. Activists are therefor limited to the digital realm while failing to address the physical impact of digital technologies and services. We will address this problem during our time together and offer some solutions that can mitigate it.

If funds usually tie the NGOs to the State, the usage of digital tools and services makes NGOs an easy prey for the big tech companies. Since the attempts of the regulators on both side of the ocean are ramping up, the companies are eager to present their "nice face", influencing NGOs to speak on their behalf or using NGOs to present themselves as the "friends of the people". This is especially dangerous as we can see in several cases that the industry is practically running the show, influencing the decision-making process and then using the collaborations with the NGOs as "proof" that they are doing the right thing.

Final question we will address during our training is the question of action and reaction. Usually NGOs are very good at reacting on legal proposals and other events in the field they cover. Government purposes a law and an NGO reacts. A crisis happens and the NGOs are there to help resolve it. But what about pro-active work and so-called awareness raising? And what is the role of the general public in connection with the NGO activities? How should you attract and maintain a relationship with the general public in order to get your message out there but also to cause ripples through-out the society?

But let us start at the beginning. Let us first take a look at the development cycle of digital policies, involved parties and the role of the NGOs in this regard. This will help us addressing the key points of the process and also inspect the best possible ways for an NGO to leave its mark on the decision-making process.

13.1. Regional digital policies – introduction into the topic

The main issue of digital environment is its supposed omnipresent characteristic of information technologies that represents a very unique way of dealing with the challenges they bring into our lives. The power dynamics of big tech companies that control this field and are very carefully placed so that they do not interfere with one another on one side and the fragmented regulators on the other side present one of the currently still unresolved challenges in this field.

Currently, the Balkan region is uniquely separated between China, USA and EU that are trying to assert dominance in this region. We will take a look at some of the specific policy cases later on, but let us first focus on the issue of the policy chain that usually happens in the region. The question we will address first is: "Where are all of these ideas coming from?"

We can agree that our countries are not the digital policy leader, not even within their own region. This stems from several reasons that we will address and examine now. The most obvious reason for our passivity of decision-makers is that countries from the Balkan region do not represent a powerful political entity that is able to manifest and enforce its own policies, but is in this regard dependent on foreign forces. Second issue is the lack of economical clout that would sway companies to consider our region as a technology hotbed. Finally – the relative low buying power of citizens living in this region represents the final nail in the coffin of policy development that is tied to the lack of economic interest of big players in this field.

13.2. Vectors of influences

Let us now examine how these three reasons influence the policy development in the region, which actors are most active in this field and how do specific policies come to life. This will help us developing effective NGO campaigns and methods of countering different tactics from these actors.

a) **Vector 1: The political conglomerates**

We can argue about the influence of politicians, but they still represent one of the key vectors of policy implementations. Government and parliaments represent key actors in this field because of one key reason – every policy should have a legal support. This is important because of two reasons: the way policies get debated in the public and second, the way policies get executed and supervised.

Goals: To establish an environment suitable for business investments, to assure the respect of human rights and to walk a thin line between different interest groups.

b) Vector 2: Private sector representatives
Big Tech companies, local businesses and other actors from private sector (lobbyists, intermediaries...) are focusing on their private interests and help influence policy development in specific countries. Their access to decision-makers and rather narrow focus of interest makes them influential and very dangerous at the same time.

Goals: To influence decision-making process and limit the impact of regulatory framework.

c) Vector 3: The public
Generally speaking the public is NGOs greatest friend and foe at the same time. Since the politicians and private sector representatives are trying to sway public opinion and get support for their agendas, the public plays the ultimate pendulum on the scale.

Goals: To live the best possible lives.

13.3. Path of a policy

So how does a policy in the realm of information society come to fruition? One of the best ways to trace the developments is to follow technological innovations from the private sector. Although they sometimes limit on science fiction, they are a good indicator of things to come.

Innovation: Since information society is consumer-driven the next step in the policy development is the implementations of technology solutions. Smart cities, 5G, biometric surveillance, data rights... all of these things are technology innovation first, techno-deterministic solutions second. Although the public discourse is mostly focusing on the latter part, we must not forget the first. These are problems in search of solutions.

Adoption: Second stage is common adoption of innovative technologies. This can happen via market mechanisms or by legal frameworks/decision by public sector. Think back on the implementation of Zoom software during pandemic, usage of Google suite tools and other cases where certain technological solutions suddenly become widely-adopted solutions.

Regulation: The third issue is regulation. This usually happens after something goes wrong after wide-range adoption and the regulators and political representatives are forced to react, either via of their own accord or via public pressure.

13.4. The shaping of techno-politics

If we use the definition of techno-politics as "hybrids of technical systems and political practices that produce new forms of power and agency", we can see the driving forces in our environment in this regard. The neoliberal pressure of business interests that are trying to legitimate its business practices and therefor require political support without any questions or opposition.

Speaking broadly, we can examine a couple of key topics that play a vital part in policy development and are at the same time the driving forces of biggest conflicts in the regional and global aspect and try and see if we can use them when developing NGO strategies.

a) Ownership of data
This is one of the key issues that can be applied to every single field, from e-health do advertising, from environment to commerce. Data ownership and practices of resolving this issue are one of the driving forces of everything that is going on in the field of digital society today.

b) Privatization of public spaces
Directly related to data ownership is the space ownership. Issues from public space ownership to the more current meta-space ownership represent another hot topic that requires political resolution and the more broader public debate.

c) Automatization of society
Workers rights and the general trend of automatization is not just relevant from the consumer's point of view but also from the point of citizens, as algorithms and other ways of automatizing different aspects of our society are marching forward.

d) Surveillance state
Combining several other issues, the surveillance state is nevertheless another trend that permeates different policies and other activities in this field. Although it stems from the ownership of data, the surveillance state is nevertheless a far more overarching issue, as it lies in the hands of those who can automatically legitimize these practices.

e) Consumerism of citizens
Finally, we reach the ultimate conglomerate – the consumerism of citizens via big data collections, algorithmization of work and surveillance state. This is leading us down a path of no return where people are limited to their consumer participation index, while every other individual's role withers away.

14. Digital activists: What do they want?

As mentioned in the morning one of the key driving factors of digital activists is their relationship with public funds and grants that exist in this field. The professionalization of this field can cause further splits between different organizations that focus on different approaches to addressing and solving the topics we've discussed previously.

The funding helps dictate the activist's manifestation and shape their approaches and topics they cover. At the same time, activist can help shape the media narrative, as they offer fresh insights into the subject that do not necessarily sync with the agendas of industry and other actors. There are two main paths that the NGOs usually take – they want to influence the decision-making process of a certain policy or they try and react on a problem that already exists in the field.

Both of the paths have some commonalities in terms of ideas representation from the NGOs, but at the same time require a completely different approach when covering these topics from the journalistic side or when trying to lead them as an NGO. I guess you could say that NGOs generally try to legitimize and open up the field of human rights in the digital sphere.

One of the biggest issues in terms of digital NGOs representations is their alignment with other actors in the field – industry and state. Before-mentioned issue of financing specific campaigns and other mechanisms of alignment are usually not investigated by the journalists and can cause cases of astro-turfing and other ways of hijacking public discussion.

As an NGO, one of the key aspects is making your ideas clear so that they resonate with the general public and the media. "Translating" global issues into local ideas and concepts can go a long way, since people are more ready to accept and ponder ideas that reflect in their local environment.

15. Digital activists: Regional campaigns

Let's take a look at three campaign examples from the region and try to analyse them from the point of focus, goal and purpose. This will help us in planning our own campaigns and preparing materials, reaching out to journalists and decide on our focus, goal and purpose. Focus can be generally understood as the field of interest, goal is something concrete and quantifiable and purpose is something more general.

15.1. EU-wide: Reclaim your face

EU-wide campaign is focusing on the issue of biometric surveillance and regulation. It involves NGOs, legal scholars, activists, people from several industries and public sector. It gathers evidence of biometric surveillance implementations, shows issues with this technologies and call for the people to react, sign a petition and force the EU decision-makers to react.

Focus: Biometric surveillance
Goal: Sign the European citizen's initiative
Purpose: Open the wide debate about biometric surveillance

15.2. Slovenia: State advertising contracts

A campaign is focusing on state advertising contracts and the way public money is funding party propaganda via advertising contracts. Activists gather documents, interview experts, examine the transparency reports and call for a parliamentary/police investigation into the matter.

Focus: State advertising contracts
Goal: Parliamentary/police investigation
Purpose: Prevent the public funding of propaganda

15.3. Serbia: City of 1000 cameras

A campaign is mapping every instance of surveillance camera installation in Belgrade, Serbia, questions the legality of the operation and tries and open up a public debate on the issue of surveillance and the political responsibility.

Focus: City surveillance system
Goal: Prevent the system from being implemented
Purpose: Question the legality of the system

16. Digital policies: Hot topics of tomorrow

Which topics are currently hot issues of digital policies and who influences the debate in the region?

a) Ownership of data This is one of the key issues that can be applied to every single field, from e-health do advertising, from environment to commerce. Data ownership and practices of resolving this issue are one of the driving forces of everything that is going on in the field of digital society today. • Advertising industry • E-health • Big tech as public service	**b) Privatization of public spaces** Directly related to data ownership is the space ownership. Issues from public space ownership to the more current meta-space ownership represent another hot topic that requires political resolution and the more broader public debate. • Smart city • Surveillance capitalism • Tech sphere of influence
c) Automatization of society Workers rights and the general trend of automatization is not just relevant from the consumer's point of view but also from the point of citizens, as algorithms and other ways of automatizing different aspects of our society are marching forward. • Robotisation of work • Platform capitalism • Algorithmic decision-making	**d) Surveillance state** Combining several other issues, the surveillance state is nevertheless another trend that permeates different policies and other activities in this field. Although it stems from the ownership of data, the surveillance state is nevertheless a far more overarching issue, as it lies in the hands of those who can automatically legitimize these practices. • Commercial biometric surveillance • Police surveillance • Global surveillance
e) Consumerisation of citizens Finally, we reach the ultimate conglomerate – the consumeration of citizens via big data collections, algoritmisation of work and surveillance state. • Social scoring • Algorithmic decision-making	

17. Conclusion

We have come to the end of our time together. Covering the surveillance capitalism from the point of personal protection as well as from the point of media discourse is one of the key topics of our society as it enables consumers and citizens to recognize their role and develop an effective strategy of countering harmful effects of it.

At the same time digital activism requires special attention as it offers new ways of engaging consumers and citizens while focusing on the decision-making processes that are one of the key tools for surveillance capitalism legitimization on one side and its limitations on the other.

By being aware of the procedural component of resistance and also diversifying your online presence, calls to action and focus on digital campaigns you will be able to recognize, address and counter harmful effects of surveillance capitalism and help in resolving this human rights issue that permeates every field of our social and private lives.