The Balance Between Surveillance and Privacy

Adjusting to a Changing Threat Landscape

Lasse Berntzen
School of Business
University of South-Eastern Norway
Horten, Norway
e-mail: lasse.berntzen@usn.no

Craig Marais
Cybersecurity Research Group
Gokstad University College
Sandefjord, Norway
e-mail: cm@gokstadakademiet.no

Abstract—**The cybersecurity threat landscape is growing dramatically, and digital surveillance and its consequence of losing privacy are among the top 10 threats. However, there are contradictory discourses regarding the purpose of surveillance, whether it is for safety or for breaching the privacy of individuals and threatening the security of society. In this paper, we unpack the concept of surveillance and its various forms and purposes. We further look at the factors that advanced surveillance practice, such as technology and the electronic footprint, in addition to the growing group of threat actors. We discuss the matter of balancing surveillance and privacy and draw insights into key measures to deal with surveillance practices by various parties to breach individuals' privacy and the security of society.**

Keywords-surveillance; privacy; human rights; electronic footprints; threat landscape; measures.

I. Introduction

This paper is a follow-up to an earlier paper coauthored by one of the authors. In that paper, Berntzen and Karamagioli focused on human rights in the context of the digital society [1]. As they observed, privacy is a fundamental human right recognized in all major international agreements regarding human rights, such as Article 12 of the Universal Declaration of Human Rights [2]. The authors emphasized the growing importance of privacy in the context of the digital society. They pointed out that citizens are possible subjects of new and powerful systems of surveillance, personal data collection, and other sophisticated Internet-based techniques, such as the use of "tracking cookies," leaving users completely unaware of such privacy breaches taking place. They also observed a change in government policies where the current political situation in the world and the threat of terrorist attacks have led to governmental proposals in the European Union requiring Internet service providers to store personal information, such as data relating to Internet traffic, e-mails, the geographical positioning of cellular phones and similar, for more extended periods than currently required [3]." They concluded that "ICT offers the technical possibilities of embedded privacy protection obtained by making technology trustworthy and legitimate by design. This includes incorporating options for socially acceptable behavior in technical systems and making privacy protection rights and responsibilities transparent to the user. Therefore, privacy should be a major concern when designing future regulatory mechanisms addressing the digital society."

The paper by Berntzen and Karamagioli [1] was written in 2008. Since then, society has changed. First, the number of electronic footprints has grown exponentially. Second, the threat landscape has changed dramatically; in a recent Delphi study report by the European Union Agency for Cybersecurity (ENISA) [4] on foresight cybersecurity threats for 2030, the threat "Rise of Digital Surveillance Authoritarianism / Loss of Privacy" is ranked number five among the top 10 prioritized threats.

Surveillance has been given several definitions, many of which fall outside the digital scope that we are concerned with, such as defining surveillance as "a systematic social practice" or "watching over and listening to personal details of people." All forms of surveillance have been used for various purposes, such as national security, policing, marketing, epidemiology, and public health [4].

This paper focuses on *digital surveillance using information technology*. This is typically concerned with the collection of personal data; this can be termed "data surveillance" or simply "dataveillance" [5]. A recent example of public health dataveillance is the mobile application *Smittestopp* (Stop the Infection) [6], developed by the Norwegian Institute of Public Health in collaboration with the Simula Research Laboratory. The app was used during the COVID-19 epidemic to track the spread of the virus within Norway and research the effect of the preventive measures applied to deal with the pandemic. However, the Norwegian Data Protection Authority "Datatilsynet" banned the processing of personal data collected by the application, rendering it practically useless.

Furthermore, the widely known Chinese social credit system [7] is an example of dataveillance, implemented as a means of building trust in society through rewards and punishments to fight corruption, telecom scams, tax evasion, academic plagiarism, and pollution, among others.

Privacy has been cited along with surveillance in various discourses, such as seeing surveillance as breaching privacy, using privacy to regulate surveillance, or using surveillance for marketing, which breaches the consumers' privacy but empowers them [5]. According to the International Association of Privacy Professionals (IAPP) [8], privacy is the right to be let alone or freedom from interference or intrusion. In contrast, information privacy is the right to have

ISBN: 978-1-68558-193-0

control over how your personal information is collected and used.

The question: “Would you prefer privacy or safety?” is relevant for most people. In a society where citizens feel unsafe due to criminal activities, terrorist attacks, and ongoing wars, many citizens welcome surveillance as a safety measure. But surveillance can be abused. One thing is government agencies surveilling public spaces or doing surveillance of criminal suspects after seeking court approval. Another thing is when private companies use the same technologies and tools to profile citizens. This prompts another question: “What is the acceptable use of surveillance?” Many citizens install surveillance equipment in their homes for safety. But that is not the same as giving others access to their homes.

This paper focuses on individuals, but individuals are mostly targets because they are part of an organization. Therefore, the organization plays an essential role in protecting its individuals, and individuals should be considered based on the organizations in which they participate.

The next section discusses the growing electronic footprints, followed by a section reviewing the current threat landscape with new threat actors in the context of surveillance. Section IV discusses how to balance surveillance with privacy. Section V concludes the paper.

II. Growing Electronic Footprints

Surveillance is more than video cameras on street corners or eavesdropping on conversations. It is also about digital footprints caused by advances in technology and new ways to collect and analyze such footprints. The following paragraphs discuss some of these footprints.

A. Smartphones

Smartphones have become an integrated part of modern life. The users may perform an increasing number of sensitive and critical tasks, making them a very lucrative target for attackers. Beretas [9] presents an overview of smartphone surveillance methods. Smartphones collect a lot of information, such as geographical position and user behavior. Positioning data is shared with service providers. Smartphones also collect other types of information, like video, photos, and speech, which can be compromised.

B. Electronic payments

Cash is less and less used. Electronic payments through smart cards or smartphone payment solutions are taking over. Each transaction is stored with, amongst other data, a timestamp, location, and amount. Lauer [10] discusses surveillance using credit and payment cards, while Martin [11] addresses digital footprints generated by mobile money.

The payment data is valuable for analyzing customer behavior and leaves digital footprints.

C. Smart Cars

Smart cars with built-in communication capabilities bring some advantages to their users. The vehicle can report on maintenance status and alert the repair facility about the problem. If the smart car is involved in an accident, the vehicle can alert emergency services automatically. But smart cars also generate comprehensive digital footprints. Claypoole [12] discusses how vehicles will continue to be more intrusive in our lives. Automatic toll stations using plate recognition or RFID technology add to the amount of information generated.

D. Surveillance cameras

The number of surveillance cameras has grown exponentially. According to Jha [13], 122.1 million households globally use security cameras. Household cameras can be hacked and may be a severe threat to privacy.

Law enforcement uses video surveillance to monitor public spaces, while companies use video surveillance to protect their properties. Video surveillance is both preventive and valuable for criminal investigations. Ashby [14] analyzed 251,195 crimes recorded by British Transport Police that occurred on the British railway network between 2011 and 2015. CCTV was available to investigators in 45% of cases and judged to be useful in 29% (65% of cases in which it was available).

E. Internet of Things (IoT) devices

According to the Norwegian newspaper Aftenposten [15], the number of IoT devices is growing and is estimated to be more than 14 billion devices globally. IoT devices represent a challenge to privacy since they may be used for surveillance of individuals and households to map behavioral patterns [15].

F. Artificial Intelligence

The vast amount of information generated by the electronic footprints can be utilized more efficiently due to the implementation of artificial intelligence to analyze numerous data streams at the same time. Feldstein [16] reported on the global expansion of AI surveillance. He mentions new possibilities to analyze digital information in smart cities/safe cities, facial recognition, and smart policing.

III. New Threat Actors and Surveillance

Since George Orwell’s novel 1984, surveillance is mainly connected to governments, the “Big Brother” kept track of its citizens. However, today, the threat landscape is more complex. Threat actors are not only the government but also criminals, industrial spies, private companies, individuals, hacktivists, and foreign governments.

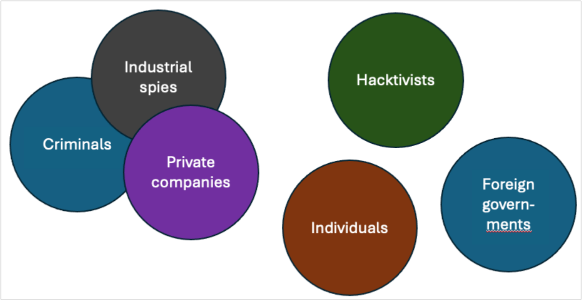

Figure 1. New threat actors.

Copyright (c) IARIA, 2024. ISBN: 978-1-68558-193-0

As shown in Figure 1, criminals, industrial spies, and private companies have overlapping motivations for using surveillance. This overlap signifies a shared motivation of financial gain, to the individual or the company. In contrast, the other actors can be seen to have motivations that differ significantly. We elaborate on these new threat actors and their differences in the following paragraphs.

A. Criminals

Criminals are driven by financial gain. They use surveillance to get information that can be used for blackmailing individuals and companies. Blackmailing may be directly connected to money, but also to gain control of or compromise individuals.

In the case of surveillance by criminals, the target victims are wealthy individuals, especially elderly wealthy individuals. Those wealthy individuals are typically lured through various social engineering techniques to gain access to their personal information and, subsequently, steal their money. Such types of threats result from the lack of awareness among those lured individuals. Consequently, this indicates the need for more regulatory and organizational measures that aim at raising public awareness.

To mitigate risks, such as threats, regulatory measures need to be in place or strengthened through creating awareness campaigns by government agencies, such as the Norwegian Center for Information Security (NorSiS), which is now part of the Norwegian National Security Authority (NSM). Examples of awareness campaigns are the banks' efforts to warn customers about phishing attacks. To support the regulatory and organizational measures, advanced intrusion detection technologies should be in place as technological measures to detect abnormal behavior based on the behavioral patterns of bank customers.

B. Industrial spies

Industrial spies are a subset of criminals with some specific goals. They want to get access to classified information that can be sold to competitors. This can be information on designs, patents, trade secrets, and marketing plans. Hou and Wang [17] observed that techniques generated by rapid developments in IoT and Data Science are enabling a massive increase in both frequency and power of industrial espionage-related activities.

Industrial spy threats are a common surveillance practice whereby an agent aims to steal trade secrets or gain a competitive advantage. This practice has gone through developments from using humans to using technology. The original form of it used to be that spies get hired as employees at the target victim organization. Those spies (under employee cover) can occupy jobs from executive management to janitors at the victim organization. The digital form of industrial spy threat is to break into computers and monitor network traffic for valuable data.

Successful industrial spy threats are a result of needing more robust internal routines for protecting company confidential information.

To mitigate the risks from such threats, organizations should establish measures to protect their infrastructure, but also do relevant background checks on employees trusted with corporate secrets.

Regulatory measures can support the protection of trade secrets through patent registrations and trade secrets laws. Technological measures could help detect break-ins and monitoring attempts.

C. Private companies

Also, private companies may engage in surveillance to get access to privacy-related information. Hinds, Williams, and Johnson [18] addressed privacy concerns and perspectives following the Cambridge Analytica scandal. Cambridge Analytica inappropriately collected data from approximately 87 million users' Facebook profiles to create psychographically tailored advertisements that allegedly aimed to influence people's voting preferences in the 2016 US presidential election [18]. The Norwegian Consumer Council expressed serious concerns about how toy manufacturers are violating privacy by collecting conversations between kids and the toys [19]. They pointed out that the toys fail at several points: lack of security, illegal user terms, kids' secrets being shared, and that kids are subject to hidden marketing.

Private companies are motivated by financial profits and can gain competitive advantages through various forms of surveillance, such as profiling of existing and potential clients, gathering intelligence on competitors, exploitive employee performance measurements, and predatory marketing techniques. Many of these techniques have existed for centuries but have become far more effective in recent years through the use of novel or improved technologies.

Counteracting these actions will require a combination of public engagement and regulatory enforcement. Governing bodies should adopt regulatory requirements for private companies, such as the General Data Protection Regulation (GDPR), in the EU and partner states.

From the consumers' perspective, they should be informed of their rights and how to enforce them when dealing with private companies. Violation of these regulations must impose meaningful penalties on the violators.

Alongside these actions, companies should be encouraged to adopt standards and compliance models that demonstrate their commitment to consumer privacy. One method for companies to establish accountability is to publish transparency reports voluntarily, these reports would help the public and third-party experts to understand how the collected data are being used.

D. Individuals

Individuals may also engage in illegal surveillance activities. Their motivation is to get access to information for personal reasons beyond blackmail and fraud. Examples can be to obtain information about the actions and whereabouts of partners, film nudity or sexual activities, or eavesdrop on conversations in the workplace based on suspicions that coworkers are badmouthing.

The availability of cheap surveillance equipment, such as hidden cameras or audio recorders, lowers the barriers for individuals to indulge in such surveillance. During Arendalsuka (Arendal week) 2024, an annual gathering for politicians, influencers, media, organizations, and other stakeholders, one of the participants is investigated after placing a hidden camera in the bathroom of a flat shared with one politician, two female colleagues, and a journalist. The camera was hidden in a portable audio speaker [20].

This example is not unique, several other incidents have been reported where individuals have placed cameras in toilets of libraries and schools, as well as locker rooms and showers in school facilities.

The legislation clearly forbids secret recordings in public spaces. However, some individuals attempt this kind of illegal behavior driven by their personal motives.

E. Hacktivists

Hacktivists often have ideological or ethical reasons for engaging in surveillance. Their motivation comes from a desire to oppose politicians and decision-makers on specific causes. They aim to reveal hidden truths, mobilize public opinion, or disrupt the operations of their targets. Examples are documenting animal abuse [21], monitoring industrial plants for contamination, or keeping surveillance of child molesters.

Hacktivists engage in surveillance to expose perceived injustices or advance their social or political agendas, often targeting governments or corporations. Many large multinational companies could be considered targets in the eyes of hacktivists; this could include large pharmaceutical companies or oil manufacturers, but hacktivists can also operate at the community level where their actions may have more immediate personal effect; they may target minorities in their community or challenge local government decisions. The common thread for the target of hacktivists is the decision-making power of the individual in the targeted organization or the social impact that ‘the hack’ will produce.

Hacktivist threats happen because of the lack of organizational measures, whether in government organizations or private organizations. Such organizations may need more plans to respond to this type of threat as well as policies to regulate similar threatening activities. In the case of hacktivists who are part of the organization, there is a high risk that they are aware of the vulnerabilities in the organization’s technological infrastructure. Therefore, the hacktivists can exploit those vulnerabilities for their own gains.

To mitigate the risks from such threats, a set of organizational measures should be in place, such as response plans that include alternative actions to handle hacktivists’ threats. Possible actions could be to engage in a dialogue with the hacktivists and try to address their legitimate concerns to resolve the conflict. Another organizational measure could be to have a policy that regulates the conduct of activist activities in a civilized way. Technological measures should be in place as well, such as advanced intrusion detection technologies in addition to cameras to observe the behavior of the hacktivists. To support the organizational and technological measures, some regulatory measures could also be employed to protect the rights of the hacktivists and the affected companies or organizations.

F. Foreign governments

Due to the geopolitical situation, surveillance by foreign governments has become more common. Foreign governments possess highly advanced technology that can be used for surveillance. Norway has seen several monitoring attempts by foreign actors targeting politicians, researchers, and industry leaders. Certain foreign technologies, especially within the telecommunications sector, have been banned due to suspicion of being used for surveillance. In March 2023, the Norwegian Ministry of Justice and Public Security decided to ban TikTok and Telegram from the work mobiles of government employees [22]. The decision was based on a recommendation from the Norwegian National Security Authority (NSM). Within a few days, other public institutions, like the Norwegian Parliament, did the same. The surveillance aims to gather intelligence to be used to blackmail or control individuals and to contribute to the destabilization of the government and political system.

To mitigate the risks of foreign government surveillance and maintain the national security of society, national governments should have in place or strengthen the organizational measures regarding counterintelligence activities to detect and disturb foreign government surveillance. Organizational measures could also include maintaining international collaboration with allied countries to share intelligence information to identify, prevent, or respond to foreign government surveillance. Regulatory measures can further support the mitigation of foreign governments’ surveillance threats through sanctions or other penalizing measures.

IV. How to Balance Surveillance and Privacy?

So far, the discussion has focused on new threat actors in the surveillance area. This section will discuss different categories of measures that can be used to balance the need for surveillance and the need for privacy. Some measures are relevant for individuals, some are relevant for organizations, and some are relevant for society at large. Figure 2 shows the organization of the society. Individuals may or may not be members of an organization, depending on the context. If they are in an organization, the organization may play a role in protecting the privacy of its individuals.

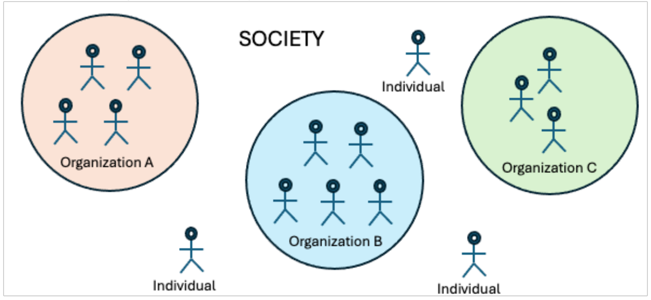

Figure 2. Different levels in the society.

Copyright (c) IARIA, 2024. ISBN: 978-1-68558-193-0

The measures may be regulatory, managerial, or technical. Regulatory measures are about laws and regulations defining the limits on surveillance and the rights to privacy for society. Managerial measures are what an organization does to protect its members. Finally, technical measures are about the use of technology to detect surveillance and protect privacy. Figure 3 shows how the different measures contribute to balancing surveillance needs with privacy protection.

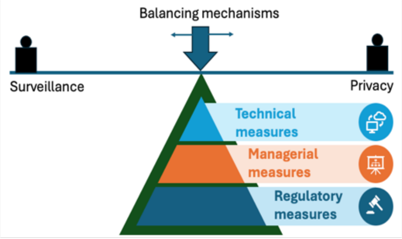

Figure 3. Balancing mechanisms.

The following subsections will describe these three categories of measures, followed by a discussion of data collection practices.

A. *Regulatory measures*

Regulatory measures regulate the use of surveillance and the protection of privacy. On the national level (society), this includes data protection laws and regulations. When deciding on the level of surveillance to be conducted, government actors must weigh up the cost (to privacy) with the proportionality of the threat. Under all circumstances, there must be a clear legal basis for the surveillance. In any circumstance where the cost is considered high, the actors must seek additional judicial oversight (such as a court order). This judicial oversight will help act as a check against potential abuse of surveillance powers. State-conducted surveillance should be done within clearly defined constraints and must stand up to legal scrutiny. New threat actors conducting illegal surveillance activities should be punished based on the severity of the misconduct. The penal code should address unlawful surveillance. On the managerial level, the organizations should comply with the regulations. Individuals should comply with the regulations and use the necessary legal mechanisms available to protect their privacy. Individuals may restrict the use of tracking cookies, not volunteer private information, be careful about using social media, and use the rights of GDPR to remove personal data.

B. *Managerial measures*

Society should protect against the new threat actors, and national authorities and agencies should be established. The police should have the necessary tools and competence to investigate illegal surveillance claims. The personnel conducting surveillance activities should be trained in both the technical aspects and the ethical considerations of their work. Ethical standards should be clearly defined, emphasizing respect for privacy and the importance of adhering to legal and procedural safeguards. On the managerial level, organizations should work on creating policies and guidelines. The most essential part for organizations is to increase their competence. The goal should be to create a security culture where they are aware of the threat landscape, potential actors, and countermeasures. Individuals also play an essential role. They should be aware of possible threats and know how to report suspicious behavior or activities (including illegal surveillance cameras).

C. *Technological measures*

The society should monitor threats and infrastructure on the national level. The national level should also communicate possible threats to organizations and, where relevant, individuals. The organizational level has an important role. Most individuals are targets because of their affiliation to an organization. The organization must secure its infrastructure by establishing relevant access control. The organization should also monitor its infrastructure with intrusion detection and intrusion prevention systems. Incident response handling should be in place, and necessary recovery mechanisms should be established. Individuals can install antivirus software and personal firewalls. They can also use secure communication through Virtual Private Networks (VPN) and avoid unsecured networks.

D. *On Data Collection*

Surveillance technologies should be designed to minimize the collection of data that is not directly relevant to the identified threat or objective of the surveillance. As it can be challenging to predict how data may be used in the future, only the bare minimum of data should be recorded during surveillance activities. Surveillance data should only be retained as long as necessary for legitimate purposes, and access to this data should be restricted to authorized personnel. At all levels, detailed records must be kept of the collection and access of surveillance data. This metadata should be easier to audit and report on and thus not jeopardize the privacy of those under surveillance. The surveillance data should be anonymized and de-identified before storage whenever possible; this helps to protect the privacy of bystanders in the case of public surveillance.

Furthermore, this data should be securely encrypted when in a storage state, further protecting the data in the event of a breach. Breaches can and do happen, and a violation of access to a system should not inherently provide complete access to all data stored therein. Technology should, by default, provide as much privacy as possible and as little access as possible; the control of one’s privacy should remain in the hands of the user.

V. CONCLUSION

The previously mentioned new threat actors find the opportunity to use surveillance for their various gains, causing a breach of privacy because of the lack of one or more of the regulatory, managerial, and technological measures. Such a lack of measures causes an imbalance between surveillance and privacy. Surveillance will always happen, but the most important thing is to ensure the protection of privacy.

Copyright (c) IARIA, 2024. ISBN: 978-1-68558-193-0

The balancing mechanisms will take place on different levels of the society. The society consists of individuals that often belong to organizations. Individuals need protection, but when they are part of an organization, the organization also has responsibilities to protect both its own and their privacy. Before engaging in surveillance, the state should do a thorough assessment to ensure that surveillance mechanisms/measures are within policy, proportionate to the threat, necessary, and the potential impact on privacy. This assessment should also account for the storage and accessing of the surveillance data generated. The public must be engaged in matters relating to the surveillance policies and practices. Public oversight bodies play a crucial role in holding their own governments and government agencies accountable for their actions and practices. They should provide guidance and possibly legal assistance to individuals who have been subject to unlawful or wrongful surveillance and thus had their privacy rights violated.

These mechanisms aim to create a balanced approach where the government can effectively protect public safety through necessary surveillance while maintaining strong safeguards to protect individual privacy. The goal is to ensure that surveillance is conducted within a framework that respects human rights and is subject to appropriate checks and balances but also protects citizens from illegal surveillance by new threat actors.

Social values do differ across borders and some populaces may be willing to allow more surveillance if they feel the benefits outweigh the cost to privacy. Our findings are influenced by a Norwegian perspective, characterized by high trust in the government alongside concerns about privacy.

References

[1] L. Berntzen and E. Karamagioli, “Human Rights in the Context of the Digital Society,” Proceedings 2nd International Conference on the Digital Society (IARIA). IEEE Computer Society, pp 129-133, 2008.

[2] United Nations, “Universal Declaration of Human Rights (1948),” [Online]. Available from: https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf 2024.08.15

[3] Commission of the European Communities, “Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC,” COM(2005)438 final, 2005 [Online]. Available from: https://www.statewatch.org/media/documents/news/2005/sep/com-438-data-retention.pdf 2024.08.15

[4] European Union Agence for Cybersecurity, “Foresight Cybersecurity Threats For 2030 - Update 2024: Executive Summary,” [Online]. Available from: https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary 2024.08.15

[5] D. Lyon. “Surveillance,” Internet Policy Review, 11(4) [Online]. Available from: https://policyreview.info/concepts/surveillance 2024.08.15

[6] J. Lund-Tønnesen, “Smittestopp (Stop the infection),” Store Norske Leksikon [Online]. Available from: https://snl.no/Smittestopp 2024.08.15

[7] Z. Yang, “China just announced a new social credit law. Here’s what it means,” MIT Technology Review. [Online]. Available from: https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean/ 2024.08.15

[8] International Association of Privacy Professionals (IAPP), “What does privacy mean?” [Online]. Available from: https://iapp.org/about/what-is-privacy/#:~:text=Broadly%20speaking%2C%20privacy%20is%20the,information%20is%20collected%20and%20used. 2024.08.15

[9] C. P. Beretas, “Smart Phones Surveillance Methods,” Journal of Clinical and Biomedical Recent Advances. 1(1), pp. 1-5, 2022.

[10] J. Lauer, “Plastic surveillance: Payment cards and the history of transactional data, 1888 to present,” *Big Data & Society*, *7*(1). https://doi.org/10.1177/2053951720907632

[11] A. Martin, “Mobile Money Platform Surveillance,” Surveillance & Society, 17(1-2), pp. 213-222, 2019.

[12] T. F. Claypoole, “How Your Car Became a Surveillance Weapon,” National Law Review, XIV(243) [Online]. Available from: https://natlawreview.com/article/how-your-car-became-surveillance-weapon 2024. 2024.08.15

[13] R. Jha, “Surveillance cameras in cities: A threat to privacy?” Observer Research Foundation. [Online]. Available from: https://www.orfonline.org/expert-speak/surveillance-cameras-in-cities-a-threat-to-privacy 2024.08.15

[14] M. P. J. Ashby, “The Value of CCTV Surveillance Cameras as an Investigative Tool, An Empirical Analysis,” European Journal on Criminal Policy and Research, 23, pp. 441-459, 2017.

[15] V. S. Wiken, «Hvor sikre er de nye smartdingsene dine? (How safe are your new smart devices),” Aftenposten. 01.08.2023. pp 4-5.

[16] S. Feldstein, “The Global Expansion of AI Surveillance,” Carnegie Endowment for International Peace (Working Paper). [Online]. Available from: https://blog.fdik.org/2019-09/WP-Feldstein-AISurveillance_final1.pdf 2024.08.15

[17] T. Hou and V. Wang, “Industrial espionage – A systematic literature review (SLR),” Computers & Security, 98, 102019, https://doi.org/10.1016/j.cose.2020.102019, pp. 1-12, 2020.

[18] J. Hinds, E. J. Williams, and A. N. Joinson, “’It wouldn't happen to me’: Privacy concerns and perspectives following the Cambridge Analytica scandal,” International Journal of Human-Computer Studies, 143, 102498, https://doi.org/10.1016/j.ijhcs.2020.102498, 2020.

[19] F. Myrstad, “Connected toys violate European consumer law,“ Norwegian Consumer Council, 2016. [Online]. Available from: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/ 2024.08.15

[20] M. Rønning and K. Skårdalsmo, “Næringstopp siktet for snikfilming under Arendalsuka (Business leader charged with surreptitious filming during the Arendal week),” [Online]. Available from: https://www.nrk.no/norge/naeringstopp-siktet-for-snikfilming-under-arendalsuka-1.17022547 2024.08.30

[21] Animal Justice Project (website) [Online]. Available from: https://www.animaljusticeproject.com/undercover-investigations 2024.08.15

[22] A. Staalesen, “Norway calls on state officials to delete Telegram,” The Barents Observer [Online]. Available from: https://thebarentsobserver.com/en/democracy-and-media/2023/03/norway-calls-state-officials-delete-telegram 2024.08.15

Copyright (c) IARIA, 2024.   ISBN: 978-1-68558-193-0