# ESSAYS I/2021

## OBSAH SEKCE



## STATE SURVEILLANCE AS THE NEW SOCIETAL NORM[1]

*TEMIRLAN BEKTURGANOV*[2]

## 1. INTRODUCTION

Privacy is an abstract term and each individual defines it in their own way, but no one can argue that privacy is not important. Surveillance has substantially developed and there are numerous conducive factors to its development. The pursuit of national security has become an acute topic and all countries joined the war on terror, however nobody raises concerns regarding its costs. We truly rely on new technologies and the matter of whether

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Surveillance. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Surveillance.

[2] Temirlan Bekturganov je studentem Fakulty sociálních studií Masarykovy univerzity, kontakt: 491700@mail.muni.cz

we are a surveillance society or not is nonsense because the answer is obvious - we are. Though, how does it affect the very idea of western values and liberal democracy? At what costs, what benefits does this notion bring about? How advanced are our technologies and how accurate are they in regards to security? These and other questions, I am aiming to examine in this paper by analyzing empirical data and inclusion of a philosophical dimension as well.

## 2. SUBJECTIVE OR OBJECTIVE SURVEILLANCE?

One of the phenomenal Greek philosophers, Aristotle, once said: humans are social animals and society is something that precedes the individual. Hence, I believe, we as individuals living in a society are constantly sharing and exchanging emotions, ideas, beliefs and values, and the main source of our emotions is coming from communications and observations on which we further develop assumptions. Society is complex and throughout the time, created complexity is substantially evolving further more. To solve problems, we increase complexity exaggerating the solution even more [3]. To elaborate on the complex society, firstly, I would like to use Gary Marx's analysis of the development of the 'new surveillance', as the solid ground of my argument, where he presents the development of surveillance in its context. Conceptualization is rooted in the religious surveillance that produced activities such as the policing of religious consciousness and created the basis for the division of 'us' and 'them', what is 'normal' and what is not. Later on, in the sixteenth and seventeenth centuries, the development was seen in terms of politics which introduced the notion - 'policed' society through observation and detection, increase in bureaucracy where data collection had become the new norm.[4] It is not my intention to dwell on the matter of the development of surveillance, but I would rather use an ex-

[3] Temis G. Taylor and Joseph A. Tainter are using an example of societal complexity by analyzing scarcity and the energy of fossil fuels, however, their explanation of the modern society, I believe, is applicable and universal to any examined topic which is related to the human activity TAYLOR, Temis G. a Joseph A. TAINTER, 2016. The Nexus of Population, Energy, Innovation, and Complexity. *American Journal of Economics and Sociology*. 75(4), pp. 1005–1043.

ample of the modern police which can be legitimately considered as an outcome of surveillance. Many scholars confidently state that humans are rational beings, though taking the example of police brutality in the U.S., I would argue that there is no such a thing as absolute rationality in human nature. The recent cases with Breona Taylor and George Floyd have only proved the fact that humans are irrational and our actions are driven by subjectivity presented in a form of assumptions. In an example noted above, the police officers' actions had led to such sorrowful outcomes just because they perceived their intentions in their own way, one may say that their actions were based on a justified belief, but all beliefs are precisely subjective. Yet, we still rely on the idea of rationalism and give up our protection and security to authorities who are responsible for the national and individual security by accepting the fact of state surveillance and justifying it with the idea of public interest.

## 3. NATIONAL SECURITY AND TERRORISM

To justify surveillance, mass media and high authorities choose to manipulate our perception of security by presenting a big impactful risk for the public, therefore they present surveillance as a tool to fight the beast for the sake of national security. What impresses me is that only a few raise questions concerning the security of an individual, yet I noticed a thought-provoking pattern of the way many perceive security by taking it as relational and drawing a correlation between national and individual security and claiming that one determines the other, though, I would argue that it is not always the case.

Indeed, surveillance is presented as a tool to solve national security issues and as we may notice, no one speaks about individual security in the framework of surveillance. The idea of national security seems tempting for the society, however, the question of costs remains neglected. To add clarity in this matter, let us look at the example of China, in particular, Xinji-

[4] MARX, Gary T., 2004. What's new about the "new surveillance"?: Classifying for change and continuity. *Knowledge, Technology & Policy* [online]. 17(1), pp. 18–37. ISSN 1874-6314. Available at: doi:10.1007/BF02687074.

ang region. One cannot deny that there is a big wave of suppression against Uighur minorities in the region and this topic is always being ignored by the international society because it concerns Chinese national security. Women's mass sterilization[5] is justifiable in a sense of national security, because it is easier to control low population insofar small number population does not entail risks for the Chinese integrity and core values (i.e. rise of nationalism and separatism). Doubtless, it is a breach of bodily privacy, violation of human rights, and is morally and ethically wrong. Hence, the argument that national security determines an individual's well-being is inappropriate and misleading.

One may argue that what if there are no violations in the privacy context exercised by the government on both individual and national levels and what if there is an actual threat of terrorist attack, how shall we expect the government not intervene into one's privacy? To answer this question, I will use Yuval Noah Harari's article on Terrorism from his book "21 lessons for the 21st century" where he claims that terrorism is no longer a major threat, but rather is a tool of mind control. Indeed, the public remembers 9/11 events as the attack on the World Trade Center, but neglects to mention the Pentagon attack because visually it is not as memorable as the former example which again proves the fact that we are of irrational nature and tend to remember events and things related to emotions caused by visually catchy images.[6] To elaborate on it and develop further analysis, I want to draw on the concept of perceived risks. Once again, as discussed in the previous section, human nature is unpredictable and we tend to make assumptions and judgements subjectively, therefore, perception of risks is not an exception. In business marketing, this concept represents uncertainty that customers encounter when purchasing goods, however, I am convinced that it is a universal pattern that also influences human's understanding and decision-making, where applying it to the perception of ter-

[5]China: Uighur women reportedly sterilized in attempt to suppress population, In: *Deutsche Welle* [online] *01.07.2020* [cit. 2021-05-26].Available at: https://www.dw.com/en/china-uighur-women-reportedly-sterilized-in-attempt-to-suppress-population/a-54018051.

[6] HARARI, Yuval Noah, 2018. *21 Lessons for the 21st Century*. 1st Edition. New York: Random House. ISBN 978-0-525-51217-2.

rorism, terrorists manipulate uncertainty that authoritive decision-makers and individuals face in a way that the issue appears to be more dangerous and serious. In point of fact, when China experienced the first wave of coronavirus back in 2019, the world remained silent because the actual risk of pandemics was never a topic and therefore no authority had come up with deliberate policies to prevent the spread of the virus, unlike, the obsessed by western powers, War on Terror which had an impact on the development of thorough representation of security, but took too much attention that in the end we ended up with weak policies towards other global threats and led to the disregard of the very idea of liberal individualism with the core values of individual rights and freedoms.

## 4. STATE SURVEILLANCE WITH NO PLACE FOR DEMOCRACY

The notion of censorship is something inappropriate and unacceptable in the 21st century in most parts of the world and is not especially admissible in the western liberal idea of democracy. It is my contention that in the world of human rights where the right for self-determination, freedom of speech and expression, mass surveillance and extra-policing in a form of a state surveillance are acute and not conducive driving forces of the democratic society, and it rather brings about the threat of the very idea of western liberalism because its core values are being disregarded. Collecting data and information beforehand of a crime carries out the so-called chilling effect which later on invokes self-censorship and chills behaviour of individuals and functioning of the whole society. I recall my mother's stories from the times she lived in the Soviet Union, where everyone was terrified and cautious of the outcomes of one's actions, in particular, it violated Article 19 of the Universal Declaration of Human Rights - freedom of speech and expression.[7] People were truly afraid of sharing their opinions with one another which led to distrust of your neighbours, friends and local communities because people knew they were being watched and it entailed social di-

[7] Universal Declaration of Human Rights. *United Nations* [online]. United Nations [cit. 2021-05-26]. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights

vision and eventually social polarization. The character of the state surveillance with advanced technologies embodies a greater scale of chilling effect, though one may argue that this effect is mainly invoked when we are certain on the fact of being surveilled, but the central problem is the uncertainty we as individuals encounter. Since we live in a Post-Snowden world, we are no longer fooled about the fact of hidden surveillance and this raises questions of transparency that democratic institutions must uphold and maintain, although, unfortunately, the reality has proven the contrary. One must admit that nowadays developments in surveillance have shifted the roles of a suspect and the government where now a subject has to prove one's innocence and not the government which is supposed to protect its citizens fairly and equally proving one's guilt. Thus, another problem concerning western values arises from here. Surveillance, specifically mass surveillance, serves as an instrument to monitor a group of individuals within which there might be a suspected subject, however, that is absolutely unconstitutional because it does not cover a certain suspect, but a group of innocent people and this regards privacy matters, as we discussed the chilling effect and self-censorship matters previously. Ideally, in a truly democratic country with the high value of rule of law, which is the U.S. in fact is, in order to find a suspect or even a guilty person, the authorities must have an issued warrant for an investigation and surveillance which is a part of an investigation, but as Edward Snowden revealed,[8] the National Security Agency warrantlessly had allowed the search for individual's personal information, data, track of communication and the usage of other surveillance tools. That was an unprecedentedly unlawful incident and an act of disrespect towards American citizens who were not aware of an ongoing surveillance program and deriving from the past experience our questioning of government's transparency has become an acute topic and the whole idea of government which used to have an obligation to uphold an order has shifted and now we encounter the reality where individuals have no

[8] BALL, James, ACKERMAN, Spencer., NSA loophole allows warrantless search for US citizens' emails and phone calls. In: *the Guardian* [online] 09.08.2013 [cit. 2021-05-26]. Available at: http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls

longer got anything to hide, though the government's activity is vice versa hidden by all 'democratic' institutions and their representatives. Hence, I believe, people have all rights to demand transparency because this is a point where democratic-backsliding might occur if all the public has yet to awake for the sake of their own privacy.

## 5. DEVELOPING OR DEVELOPED TECHNOLOGIES?

As I already touched upon the topics of the society, complexity created and subjectivity, I must mention they all are obviously related to humans. Though, equally relevant to the issue are the questions of surveillance technology development. It is no secret that humans are now being replaced by algorithms, patterns and artificial intelligence mechanisms because this is the complexity we have created in order to ease our lives, however, I believe that nowadays technologies are not sufficiently advanced to feel reliance on. Roger Clarke draws the line between data and information where data is a component of which information consists and I would like to illustrate this point in a form of variables to elaborate further on it.[9] Data is an independent variable where information is dependent, hence data can be manipulated and interpreted in numerous ways and Clarke introduces at this point the notion of digital persona and its negative impact on the outcome where in an investigation all decisions and actions are being made on an inaccurate representation of a subject. This is not only the case of policing wrong suspects, but it also covers other social dimensions, to be precise, the matter of racism which only escalates already existing systemic discrimination. Facial recognition has proved to be imprecise when it comes to identifying people of colour which may lead to policing wrong suspects and as a result to detention while the actual criminal is free and is capable of committing a more serious crime.[10] In a sense of systemic racism, if these technologies are allowed for police use, it is by no doubt a systemic discrimination of minorities and again challenges the whole idea

[9] CLARKE, Roger. Introduction to Dataveillance and Information Privacy. In: *Roger Clarke's Web-Site* [online] [cit. 26.05.2021]. Available at: http://www.rogerclarke.com/DV/Intro.html

of western liberalism. In addition to that, reliance on algorithms and artificial intelligence is fraught with consequences that are not reasonable. As discussed in the first section, we all have a tendency to make only subjective assumptions and subjectivity also means that we question the other side of the coin whenever we have more information on a certain case, that is to say, if an investigation being led by a human, the more information an investigator has, the more questions appear consequently whereas if an investigation relied on technology and it allowed one systemic error, it will entail a negative result and may change or mislead the whole character of an investigation.

## 6. CONCLUSION

Having examined the idea of state surveillance, privacy concerns, advantages and disadvantages of the so-called advanced technologies and its relation to the usage of such aspects by irrational human beings, I arrived at the conclusion that the state surveillance has its up and down sides, at the beginning it had facilitated the war on terror and strengthened national security, though such pursuit has led to undermining the individual dimension of security. But human nature is unpredictable and as we have seen the shift of state surveillance becoming a new norm violating the very idea of liberalism which has its feature to chill societies and their ability to function properly. Mass surveillance has proved its efficiency and yet again, we have created complexity in which the solution of a problem emerges only after making it even more complex. The central issue is that there are no alternatives to surveillance with its all external obstacles and disadvantages, hence in order to come up with the alternative solution to it, we must not only change and develop new institutions controlling surveillance, but promote a new approach and novelties such as the creation of a whole new governing system, but so far, unfortunately, all we can do is only protect

[10] HARVELL, Drew. Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use. In: *Washington Post* [online]. [cit. 2021-05-26]. ISSN 0190-8286. Available at: https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

our privacy and speak up to stimulate massive awareness of the current issue and only when the entire society is awakened, we must seek for a deliberate solution in this regard.

## 7. BIBLIOGRAPHY

[1] TAYLOR, Temis G. a Joseph A. TAINTER, 2016. The Nexus of Population, Energy, Innovation, and Complexity. *American Journal of Economics and Sociology*. 75(4), 1005–1043. Available at: https://ideas.repec.org/a/bla/ajecsc/v75y2016i4p1005-1043.html

[2] MARX, Gary T., 2004. What's new about the "new surveillance"?: Classifying for change and continuity. *Knowledge, Technology & Policy* [online]. 17(1), 18–37. ISSN 1874-6314. Available at: doi:10.1007/BF02687074

[3] China: Uighur women reportedly sterilized in attempt to suppress population, In: *Deutsche Welle* [online] *01.07.2020* [cit. 2021-05-26].Available at: https://www.dw.com/en/china-uighur-women-reportedly-sterilized-in-attempt-to-suppress-population/a-54018051.

[4] HARARI, Yuval Noah, 2018. *21 Lessons for the 21st Century*. 1st Edition. New York: Random House. ISBN 978-0-525-51217-2.

[5] UNITED NATIONS. Universal Declaration of Human Rights. *United Nations* [online]. United Nations [cit. 2021-05-26]. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[6] BALL, James, ACKERMAN, Spencer., *NSA loophole allows warrantless search for US citizens' emails and phone calls*. In: *the Guardian* [online] 09.08.2013 [cit. 2021-05-26]. Available at: http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls

[7] CLARKE, Roger. *Introduction to Dataveillance and Information Privacy*. In: *Roger Clarke's Web-Site* [online] [cit. 26.05.2021]. Available at: http://www.rogerclarke.com/DV/Intro.html

[8] HARVELL, Drew. *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use.* In: *Washington Post* [online]. [cit. 2021-05-26]. ISSN 0190-8286. Available at: https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

# DO YOUTUBERS HAVE A RIGHT TO PRIVACY?[1]

*ONDŘEJ BOŽÍK*[2]

## 1. INTRODUCTION

Access and also approach to a person's privacy have changed noticeably recently, and one of the most affected groups of people by this trend are unarguably YouTubers. In this work, my goal is to give my opinion on the privacy of YouTubers and provide convincing information on which I based my opinion.

We should obviously not forget that being a YouTuber is a job like any other, and no one's not forced to do it in the sense of article 26 of the Charter of Fundamental Rights and Freedoms. Of course, with this job comes a certain risk - YouTubers are a more vulnerable group of people when it comes to their privacy, like actors, writers, musicians, or politicians (even though the question of public officials is more complicated in the sense that the public has the right to know about certain acts of official that contributes to public debate).[3] Privacy, as we already know, has a lot of aspects. In this case, I'm going to use Roger Clarke's division of privacy, which has 4 dimensions: privacy of the person, the privacy of personal behaviour, the privacy of personal communications, and the privacy of personal data.[4] In my opinion, the biggest interference is in the field of informational privacy, which covers both privacy of personal communications, the privacy of personal data and privacy of personal experience. Of course, it will depend on

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Free Speech and Media law. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Free Speech and Media law.

[2] Ondřej Božík je studentem Právnické fakulty Masarykovy univerzity. Kontakt: 480493@mail.muni.cz.

[3] See Judgement of 24.6.2004 case n. 59320/00, von Hannover v. Germany, ECHR.

[4] CLARKE, Roger. Introduction to Dataveillance and Information Privacy. In: *Roger Clarke's Web-Site* [online] [cit. 30.10.2020]. Available at: http://www.rogerclarke.com/DV/Intro.html

which content the YouTuber is providing, but in general, YouTubers are more likely to share personal things with their viewers, than their address, to which restaurant they are going on a dinner with their spouse etc. As Karoliina Talvitie-Lamberg says in her dissertation work, key factors in the interaction between YouTubers (or vloggers in general) and their viewers are confessions (when the more intimate things you share, the more success you get (not always though)), self-disclosure, and honest self-representation.[5] This trend is based on the fact, that lately, they protect more bodily privacy (privacy of the person in Roger Clarke's division), than informational privacy. The goal for YouTubers is then to achieve an ideal border of (in)accessibility, as Slavík stated in his work.[6] That means, to control the amount and nature of the information that they share. People share tons of information with the outer world daily, and in a YouTubers' case, this phenomenon is even more perceptible. This is caused by the ubiquity of their content. Their job is based on a simple equation, in which the more views you get, the more money you make. Let's imagine a situation, in which you are a YouTuber and streamer with 5 million subscribers on YouTube and 1 million followers on Twitch. On the bright side, you get tons of money out of this, pleasant, not hard, job. But the dark side of this coin is, that this fame you got by sharing things with your viewers, they get more and more curious, and start intervening into the dimension of privacy, to which you don't want to let them go. These are more precisely fields of the intimate and personal zone (bodily privacy, spatial privacy, intellectual privacy, and decisional privacy in the division of Bert-Jaap Koops et. al.).[7] Shortly, the more people you let in your privacy, the bigger is the risk of someone abuses it. The risk is not only in the fact that your personal data are shared daily with thousands of people but also in the fact that the

[5] TALVITIE-LAMBERG, Karoliina. *Confessions in Social Media : Performative, Constrained, Authentic and Participatory Self-Representations in Vlogs, Dissertation thesis*. The University of Helsinki, Faculty of Social Sciences, Department of Social Studies, Communication. p. 8.

[6] SLAVÍK, Lukáš. *Význam soukromí pro mladé aktivní YouTubery a YouTuberky*. 2018, Masarykova univerzita, Fakulta sociálních studií. p. 25.

[7] KOOPS, Bert-Jaap et al. A Typology of Privacy. *University of Pennsylvania Journal of International Law*. 2017, vol. 38, n. 2.p. 2.

people watching are storing your digitized personal data, in all circumstances, all the time.

## 2. EXAMPLES

As the first example, I would show a video of PewDiePie, who has one of the biggest channels on YouTube, in which he asks his fans not to come to his house and invade his privacy (a right to be let alone, in this sense).[8] As the first deterrent example, there is a case of Mag Turney and Gavin Free, both YouTubers living in Austin, whose house was at night invaded by one of their fans, who was armed.[9] The fan was obsessed with Gavin Free and didn't want him to have children with Mag Turney. The fan was shot that night in a collision with police. That was a clear example of when the invasion of their privacy was out of control and certainly illegal. The second example has more to do with the mental health of the person making videos for millions of people. This is the case of Reckful, a well-known streamer and YouTuber of World of Warcraft and other games, who committed suicide this year. The reason why he committed suicide was long time depression, besides caused by the pressure from his supporters.[10] When I mentioned above that YouTubers are more vulnerable than any other group when it comes to privacy, I did not mean only their fame and huge fan base. The fact that they are YouTubers, spending hours and hours in front of the computer, is also an important fact. This type of people often has a reason, why the person likes being home, in his comfort zone, in front of the computer. This reason can be often based on depression, obsession, or other mental illnesses. That's also why I gave Reckful's example. This type

[8] Reportedly, the whole school classes were going on a trip to look at PewDiePie's house. Viz PERRY, Alex. *The biggest star on YouTube wants people to stop coming to his house* In: *Insider* [online] [cit. 22. 6. 2021]. Available at: https://www.businessinsider.com/pewdiepie-wants-people-to-stop-coming-to-his-house-2016-8

[9] KIRCHER, Madison Malone. *YouTube Couple Hides in Closet After Armed Fan Breaks Into House* In: *Newyork Intelligencer* [online] [cit. 30.10.2020]. Available at: https://nymag.com/intelligencer/2018/02/armed-fan-killed-after-breaking-into-youtube-couples-house.html.

[10] ELLIOT, K. Josh. *'RIP Byron': Pro 'Warcraft' gamer Reckful dies at age 31 - National* In: *Globalnews.ca.* [cit. 18.06.2021]. Available at: https://globalnews.ca/news/7134883/byron-reckful-bernstein-death-warcraft/.

of people is certainly even more vulnerable when it comes to their privacy. There is also a fitting article in the Economist about the mental health of gamers etc: *„And games become the destructive vice of choice for some sets of players, taking the place of drugs or alcohol in a tragic but familiar narrative. But the game is a symptom of some broader weakness, sometimes of character, occasionally of mental health – and, perhaps, of society too.“*[11] Even though he is not a YouTuber because he didn't choose it as his job, I would also like to shortly talk about the Star Wars Kid, whose story also slightly touches this issue. His video, which he never intended to publish, went viral in 2003. Later on, he started getting a lot of great responses, but sadly, also a lot of very bad ones. The responses were so harsh, that he had to seek help from a psychologist, and suffered from depression and bullying at his school. As an example, he was getting letters saying he should commit suicide etc.[12] He was one of the first victims of a new type of bullying called *cyberbullying*. This type of bullying is closely connected to the invasion of YouTubers privacy when in worse scenarios, the bullies go and search the YouTuber's address and harass them personally, and sadly, this phenomenon is even more popular among young YouTubers. We have a worldwide famous young YouTuber here, in the Czech Republic, called Misha, who even made a popular song about cyberbullying that he was object to.[13]

YouTubers are often active on all possible social networks. In that order, the next big risk is, that they can be victims of hackers. Hackers then can either steal some sensitive information or, more often, ask via some social network supporters of a YouTuber for money. That happened in July 2020, when hackers attacked the accounts of Bill Gates, Jeff Bezos and Elon Musk, and asked their followers for money with a promise, that when they

[11] AVENT, Ryan. Escape to another world In: *The Economist* [cit. 30.10.2020]. Available at: https://www.economist.com/1843/2017/02/27/escape-to-another-world.

[12] HAWKES, Rebecca. Whatever happened to Star Wars Kid? The sad but inspiring story behind one of the first victims of cyberbullying. In: *The Telegraph* [cit. 30.10.2020]. Available at: https://www.telegraph.co.uk/films/2016/05/04/whatever-happened-to-star-wars-kid-the-true-story-behind-one-of/.

[13] CYBERBULLY CHANNELS ARE CANCER!!! (Leafy, Pyrocynical, RiceGum, KeemStar, etc...) In: *YouTube* [cit. 18.06.2021]. Available at: https://www.youtube.com/watch?v=rV-ijcP6vDM&ab_channel=Misha%2FMishovysilenosti.

send money, they will get twice the amount from the businessmen. In the YouTube world, in the same month this year, the account of a famous Indian YouTuber CarryMinati was hacked, asking his viewers for bitcoins.

## 3. CONCLUSION

According to the examples I provided, Youtubers are definitely a very sensible group of celebrities, whose risk is even higher due to their impact on the digital world. Of course, we could argue that it is their job, that they have chosen, but nonetheless, it deserves the full protection of one's privacy than any other. In my opinion, the key is to control the border of (in)accessibility, which guarantees that viewers will be able to see and collect just that type of data, that a YouTuber wants to share, in order to keep the data they don't want to share out of their sight.

## 4. BIBLIOGRAPHY:

[1] AVENT, Ryan. Escape to another world. In: *The Economist* [online] [cit. 30. 10.2020]. ISSN: 0013-0613. Available at: https://www.economist.com/1843/2017/02/27/escape-to-another-world

[2] CLARKE, Roger. *Introduction to Dataveillance and Information Privacy*. In: *Roger Clarke's Web-Site* [online] 1997 [cit. 30.10.2020]. Available at: http://www.rogerclarke.com/DV/Intro.html

[3] ELLIOT, K. Josh. 'RIP Byron': Pro 'Warcraft' gamer Reckful dies at age 31 - National In: *Globalnews.ca.* [online] [cit. 30.10.2020]. ISSN: 1281-3508. Available at: https://globalnews.ca/news/7134883/byron-reckful-bernstein-death-warcraft/

[4] HAWKES, Rebecca. Whatever happened to Star Wars Kid? The sad but inspiring story behind one of the first victims of cyberbullying. In: *Telegraph.co.uk.* [cit. 18.06.2021]. Available at: https://www.telegraph.co.uk/films/2016/05/04/whatever-happened-to-star-wars-kid-the-true-story-behind-one-of/

[5] KIRCHER, Madison Malone. *YouTube Couple Hides in Closet After Armed Fan Breaks Into House* In: *NewYork Intelligencer* [online] [cit. 30.10.2020]. ISSN: 0160-2896. Available at: https://nymag.com/intelligencer 2018/02/armed-fan-killed-after-breaking-into-youtube-couples-house.html

[6] PERRY, Alex. *The biggest star on YouTube wants people to stop coming to his house* In: Insider [online] [cit. 22. 6. 2021]. ISSN 2225-2592. Available at: https://www.businessinsider.com/pewdiepie-wants-people-to-stop-coming-to-his-house-2016-8

[7] SLAVÍK, Lukáš. *Význam soukromí pro mladé aktivní YouTubery a YouTuberky*, bachelor thesis, Faculty of Social Studies, Masaryk University. [online]. 2018 [30. 10. 2020]. Available at: https://is.muni.cz/th/n55m5/ .

[8] TALVITIE-LAMBERG, Karoliina. *Confessions in Social Media: Performative, Constrained, Authentic and Participatory Self-Representations in Vlogs*. Dissertation thesis. 2014. The University of Helsinki, Faculty of Social Sciences, Department of Social Studies, Communication. [cit. 30.10.2020]. Available at: https://helda.helsinki.fi/handle/10138/44901

[9] CYBERBULLY CHANNELS ARE CANCER!!! (Leafy, Pyrocynical, RiceGum, KeemStar, etc...) - YouTube. In: *YouTube.com* [cit. 30.10.2020]. Available at: https://www.youtube.com/watch?v=rV-ijcP6vDM&ab_channel=Misha%2FMishovysilenosti

[10] Judgement of 24.6.2004 case n. 59320/00, von Hannover v. Germany, ECHR, CE:ECHR:2004:0624JUD005932000, Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-61853%22]}

---



---

# THE LIMITS OF JOURNALIST'S SOURCE PROTECTION[1]

*BARBORA BŘEŽNÁ*[2]

## 1. INTRODUCTION

In this essay, I would like to discuss the importance of free press as a watchdog and the obligation to protect sources and its limits. As this topic includes a variety of issues worth discussing, I will narrow it down to only few of them and I will not discuss the „private" matter any further, and by „private" matter I mean disputes between journalists and ordinary people or celebrities affected by the press (such as the case of Bladet Tromso and Stensaas v. Norway)[3]. This essay will limit its focus on the role of free press as a watchdog of politicians and democracy as such and its importance in general, instead.

The privileged position of media derives from the view that political expression plays central role in democratic society. In general, it is more acceptable to use severe and harsh criticism targeted at politicians and political matter as the freedom of expression is of vital importance in this case. Much less protection is granted to the privacy and reputation of politicians, particularly in cases when obtained information, no matter how personal, has an impact on their duties and public functions.[4] Therefore, there is no

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Free speech and media law. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Free speech and media law.

[2] Mgr. Barbora Březná je studentkou Právnické fakulty Masarykovy univerzity. Kontakt: 460108@mail.muni.cz.

[3] Amicus Curiae Opinion on the Relationship between the Freedom of Expression and Defamation with Respect to Unproven Defamatory Allegations of Fact as Requested by the Constitutional Court of Georgia [online]. Council of Europe. 2004. p. 19 [cit. 18. 6. 2021] Available at: https://www.venice.coe.int/webforms/documents/CDL-AD(2004)011-e.aspx.

[4] BYCHAWSKA-SINIARSKA, Dominika. Protecting the right to freedom of expression under the European Convention of Human Rights [online]. Council of Europe. 2017.p. 64. [cit. 18. 6. 2021] Available at: https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814.

doubt that the activities of the minister of health, such as visiting a closed restaurant with another public figure, will not be protected under the right to privacy, but supposedly celebrating an anniversary with his wife should be protected.

According to the judgement of the Grand Chamber, there is a fundamental distinction between reporting facts (which includes even controversial ones), that may contribute to public debate in democratic society relating to politicians in the exercise of their functions, and reporting of details of private life of an individual who does not exercise official functions.[5] It is important to add that public interest as such should not be a mere "interested public", but should go beyond that.

## 2. THE COLLISION OF SOURCE PROTECTION AND PUBLIC INTEREST

When protection of privacy and protection of media are confronted, none of them takes preferences automatically. It is needed to balance the protection of each of them in particular cases.[6]

In my point of view, media and free press are very powerful tools. In democratic society, they must be allowed to investigate affairs, provide people with information about how public figures and politicians fulfil their duty that have been entrusted to them, how they manage public finances, who they meet with, and many others. This requires a great deal of funds and financial resources to support such media. This had become increasingly difficult some time ago with media publishing a lot of its content for free (such as idnes.cz and others). This development has taken a turn lately, and it is slowly becoming normal again to pay for high-quality content and news coverage (e.g. Deník N, Hospodářské noviny and many others).

---

[5] SMITH, Robin Callender. *F*rom von Hannover (1) to von Hannover (2) and Axel Springer AG: Do Competing ECHR Proportionality Factors Ever add up to Certainty. *Queen Mary Journal of Intellectual Property*. [online].2012. Vol. 2, p. 390. [cit. 18. 6. 2021] Available at: https://heinonline.org/HOL/P?h=hein.journals/qmjip2&i=389.

[6] *WESTKAMP, Guido.* Private Life and the Margin of Appreciation, Introductory Note to the European Court of Human Rights: Alex Springer AG v. Germany and Von Hannover v. Germany (No. 2). *International Legal Materials.* [online].2012 *Vol. 51, p. 633.* [cit. 18. 6. 2021] Available at: https://heinonline.org/HOL/P?h=hein.journals/intlm51&i=677.

Furthermore, politicians are now granted additional space to address issues on their own in the form of social media. Prime Minister Andrej Babiš, Minister of Interior Jan Hamáček, Minister of Health Roman Prymula (who was the Minister of Health at least at the time when this essay was written), and many other important politicians, ministers and leaders are active on social platforms, e.g. Facebook and Twitter. They can address their followers and fans directly, without the "help" of media. Therefore, they are able to debunk many allegations themselves right away, they can explain the matter from their perspective immediately when something happens or they can simply get in touch with their voters. This, in my point of view, also weakens the position in which the media and newspaper are nowadays a little bit. They are not per se needed by politicians themselves, who can share a fair amount of their content for free online instead, but media and free press, on the other hand, need finances in order to perform their duty as a watchdog of a democratic society.

Many of the affairs that are made public would not be known without a reliable source (often very close to the politicians in particular), who confides details about particular affairs in journalists or who keeps informing them about it afterwards. This may be controversial, as the source should stay anonymous and, in most cases, his identity is never revealed to public.

The sources of information are protected under Article 10 of European Convention of Human Right. The article states that exercise of freedom of expression may be subject to formalities, conditions, restrictions or penalties as are prescribed by law in the interest and for preventing the disclosure of information received in confidence.[7] This protection of journalistic sources is one of the basic conditions of freedom of the press, otherwise (and without granted protection), sources may be discouraged from assisting the press in informing the public on matters of public interest, which, as a result, may weaken and undermine the vital public watchdog

[7] Article 10 section 2. European Convention on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16 [online]. [cit. 18. 6. 2021] Available at: https://www.echr.coe.int/documents/convention_eng.pdf.

role, because the ability of the press to provide reliable information may be adversely affected.[8]

One of the cases in which the protection of source is discussed is the case of Goodwin v. the United Kingdom. Mr Goodwin, who was a journalist, received information from his source by telephone. The source informed Mr Goodwin that the company Tetra Ltd. was about to raise a large loan while it had major financial problems. When Mr Goodwin called the company to get additional information for his article, Tetra Ltd. requested he reveals the source of information. They argued that this would help them with identifying dishonest employees and later with initiating proceedings against them.

In this case, the European Court of Human Rights ruled that protection of journalistic sources is one of the basic conditions for press freedom and the lack of protection may potentially result in chilling effect, therefore affecting the freedom of expression. Such revelation would violate the freedom of expression.[9]

Additionally, in Sanoma Uitgevers B.V. v. Netherlands[10] it was ruled by the Grand Chamber that "*orders requiring journalists to disclose their sources must be subject to the guarantee of judicial review or review by another independent and impartial review body*." Also, criteria for such review were identified as follows. Such body should be independent and separated from the executive branch and other interested parties. Power to determine whether public interest overrides the protection of journalistic sources should be vested in such body prior to the handing over of such material. Also, it should prevent unnecessary access to information capable of disclosing the sources' identity. Such body should have clear criteria, that also include whether a less intrusive measure may be sufficient. The fact that the review of material takes places only after the material was handed over, and such material may reveal the source, can undermine the essence of the right to

[8] BYCHAWSKA-SINIARSKA, Dominika. opt. cit., p. 100.

[9] Ibid.

[10] Judgment of the ECHR of 14 September 2010, appliaction *no*. 38224/03, Sanoma Uitgevers B.V. v. Netherlands, para 90-92.

confidentiality, therefore, it should take place prior to this. In addition to this, potential risks and respective interest must be weighted prior to any disclosure. Also it should be possible for the judge (or any other authority) to refuse to make a disclosure order and protect sources from being revealed, and to do so whether or not they are specifically mentioned in the withheld material, if the communication of such material creates a risk of compromising and revealing the identity of journalists' sources. Last but not least, there should be a procedure to identify information potentially leading to the identification of the source in urgent cases, and isolate those information from information that do not carry such risk, so the material is not exploited by the authorities.[11]

The courts of the Czech Republic also had to deal with the protection of the source. In this case, journalist Martin Šmok was ordered to pay a fine for refusing to identify and reveal the source of published information to the police and the prosecuting authorities, who were investigating the crime reported by the source. The Constitutional Court of the Czech Republic held that Martin Šmok should not had been ordered to pay the fine and deciding otherwise was violating the freedom of expression. In this case, the police and prosecuting authorities should have found alternative ways of identifying the source or obtaining the required information. The course of action adopted by police and prosecuting authorities was unlawful, according to the Constitutional Court.[12]

This is not the only case in the Czech Republic when journalist protecting its source was being punished for doing so. Similarly, in 2000, two journalist, Sabina Slonková and Jiří Kubík, were prosecuted on the initiative of Miloš Zeman, who was the prime minister at the time, because they refused to reveal the source of the information in so called "Olovo" affair. This, at the time, concerned Miloš Zeman and Petra Buzková, his rival and member of the same party, who had become increasingly popular with his voters. The team surrounding Miloš Zeman had plans to discredit Buzková and damage her reputation. When Slonková and Kubík made the whole af-

[11] *BYCHAWSKA-SINIARSKA, Dominika.* opt. cit., p. 102.

[12] Judgement of the Consitutional Court, 27th September 2005, I. ÚS 394/04.

fair public, they refused to reveal the source of the information. In return, Miloš Zeman initiated their prosecution. Fortunately, both journalists were granted pardon from Václav Havel, so this matter was not dealt with any further (by courts).

However, the protection of source related to the freedom of expression is not absolute or endless. There may be (and should be) cases, when this particular freedom is outweighed by something else. It is needed to balance the rights, freedoms and duties in specific cases, so that everyone's freedom may be exercised to its guaranteed and fullest extent. The journalists and their sources are not stripped of certain lawful duties. For example, they are obliged to inform the police and prosecuting authorities if they come to know that criminal act is about to happen.

## 3. CONCLUSION

In general, it is needed that the public interest on disclosing and revealing the source is strong enough and that it outweighs the freedom of expression (which of course may happen in certain cases). Also, the Constitutional Court in the case of Martin Šmok held that it may be permissible to reveal the source of information to the prosecuting authorities if the case is connected with particularly serious criminal act and there is no alternative for the prosecuting authorities to gain required information. However, this means that the prosecuting authorities cannot just go "the easy way" (as they often do) and try to force the journalist to reveal the source and in case he does not comply, order him to pay a fine. But, as was held, and as the common rule is, the freedoms have to be balanced and the freedom of expression may be exercised to a certain extent – until it is outweighed by something of greater importance.

## 4. BIBLIOGRAPHY

[1] BYCHAWSKA-SINIARSKA, Dominika. Protecting the right to freedom of expression under the European Convention of Human Rights [online]. Council of Europe. 2017.p. 64. [cit. 18. 6. 2021] Available at: https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814.

[2] European Convetnions on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16 [online]. [cit. 18. 6. 2021] Retrieved from: https://www.echr.coe.int/documents/convention_eng.pdf.

[3] SMITH, Robin Callender. From von Hannover (1) to von Hannover (2) and Axel Springer AG: Do Competing ECHR Proportionality Factors Ever add up to Certainty. *Queen Mary Journal of Intellectual Property*. [online].2012. Vol. 2, pp. 389–393. [cit. 18. 6. 2021] Retrieved from: https://heinonline.org/HOL/P?h=hein.journals/qmjip2&i=389.

[4] Amicus Curiae Opinion on the Relationship between the Freedom of Expression and Defamation with Respect to Unproven Defamatory Allegations of Fact as Requested by the Constitutional Court of Georgia [online]. Council of Europe. 2004. [cit. 18. 6. 2021] Retrieved from: https://www.venice.coe.int/webforms/documents/CDL-AD(2004)011-e.aspx.

[5] *WESTKAMP, Guido.* Private Life and the Margin of Appreciation, Introductory Note to the European Court of Human Rights: Alex Springer AG v. Germany and Von Hannover v. Germany (No. 2). *International Legal Materials.* [online] *2012, Vol. 51, pp. 631–684.* [cit. 18. 6. 2021] Retrieved from: https://heinonline.org/HOL/P?h=hein.journals/intlm51&i=677.

[6] Grand Chamber Judgment of the ECHR of 14 September 2010, appliaction *no*. 38224/03, Sanoma Uitgevers B.V. v. Netherlands.

[7] Judgement of the Consitutional Court, 27 of September 2005, I. ÚS 394/04, N 184/38 SbNU 471.

---



---

# THE DANGERS A SMART HOME AND HOW TO AVOID THEM[1]

*MARTIN BUKOVIČ*[2]

## 1. INTRODUCTION

In this work, I will deal with the issue of smart homes. My main task will be to deal with one of the biggest pitfalls of smart homes, which is security. My research question, which I will try to answer, is, what are the security risks of smart homes and how to avoid these security risks? Directly related to this is the question of which devices of smart homes are the biggest security threat? I should find the answer to these questions in this work.

I will first define the term "smart home". I will define the specifics of what can be considered a "smart home". Acquiring a smart home is also related to the benefits that the smart home itself brings to its users. However, on the other hand, there are many disadvantages that a smart home brings. This is also related to security risks, which I will address in connection with the smart home in the next part of this work. I'll look at some smart devices in a smart home and explain how their security can be broken. I will explain the danger of an unwanted attacker infiltrating one of the smart devices connected to the smart home. In the last part of this work, I will try to clarify how to prevent this infiltration of attackers into the smart home. The work should provide a suitable guide on how to avoid mistakes when purchasing a smart home and thus have your home under your control.

## 2. WHAT IS A SMART HOME?

First, I will define the term “smart home”, which is the main topic of this work. The smart home concept is being used by more and more people.

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Smart everything. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Smart everything.

[2] Martin Bukovič je studentem Právnické fakulty Masarykovy univerzity. Kontakt: 468344@mail.muni.cz.

This is mainly due to its simple remote control from anywhere with an internet connection via a mobile phone, tablets or another similar networked device.[3] So for example, you can switch off the heating with your phone during holidays. Smart home includes automatic systems that allow residents of a house or an apartment to better control and monitor appliances, devices and the building itself. Thanks to the smart home, you can control, for example, lighting, heating, opening windows and doors, shading blinds, controlling security cameras, airflow, the refrigerator and much more. For example, how does a smart refrigerator work, if it is connected to a smart home system? It can evaluate its contents, point to an upcoming expiration date, recommends healthy alternatives, or even if some products are consumed, the refrigerator will create and send you a shopping list all by itself.[4] It can also plan meals based on the food inside your refrigerator.[5]

Smart home devices are connected and can be controlled and accessed using a central device (smartphone, central home unit etc.). A smart home thus consists of smart devices that together form one common unit, which relieves many households of worries. E.g. the smart home system handles routine matters that would otherwise be performed by the residents of the household themselves. One of the popular benefits of a smart home is that it helps create a safe home. Residents of households can secure their homes with wireless cameras, alarms, smart locks etc. Smart sensors can easily detect water or gas leaks when in case of such danger the household resident is immediately warned using a smartphone.[6]

Energy efficiency, which is very closely linked to economic savings, is one of the most important reasons why people choose to upgrade their

---

[3] CHEN, James. Smart Home. In: *Investopedia* [online] [cit. 08.01.2020]. Available at: https://www.investopedia.com/terms/s/smart-home.asp

[4] What is a Smart Home? - Smart Home Energy. In: *Smarthomeenergy.co.uk* [online]. [cit. 08. 01. 2021]. Available at: http://smarthomeenergy.co.uk/what-smart-home

[5] All Samsung Family Hub Features | Samsung US. In: *Samsung Electronics America* [online] [cit. 08. 01. 2021]. Available at: https://www.samsung.com/us/explore/family-hub-refrigerator/apps/

[6] How a smart home can improve your home security. In: *Hestiamagazine.eu* [online]. 2021 Hestia Magazine [cit. 24. 06. 2021]. Available at: https://www.hestiamagazine.eu/how-a-smart-home-can-improve-your-home-security

homes to smart homes. With smart home appliances, homeowners can control their energy consumption well enough without having to pay extra unnecessary expenses. For example, they can set the lights to turn on automatically when they enter a room.[7] There are, for example, motion sensors that can ensure that the devices will only be active if there are people in the room. Intelligent blind control can automatically maintain the room temperature without the need to turn on the air conditioner. In addition to electricity consumption, the smart home also enables controlled water consumption, where there are intelligent shower-heads or toilets that save water consumption. However, there are many more devices that can be used in a smart home. [8]

According to the Strategic Energy Technology Plan, "smart homes" were one of the agreed strategic targets in the area of smart solutions for energy customer.[9] Smart households play a very important role in the European Union's energy system. The European Commission claimed that individuals and communities have an interest in managing energy consumption, and that is why it is necessary to "*create technologies and services for smart homes that provide smart solutions to energy consumers*".[10]

## 2.1 WHAT ARE THE PITFALLS OF A SMART HOME?

Despite its many advantages, a "smart home" also has a number of disadvantages that can be very dangerous for its users. One of the primary disadvantages of getting a smart home is that it can be quite expensive. Of course, you don't have to invest that much in a smart home, but you have

---

[7] 7 Greatest Advantages of Smart-Home Automation. In: *Bluespeedav.com* [online].[cit. 08. 01. 2021]. Available at: https://bluespeedav.com/blog/item/7-greatest-advantages-of-smart-home-automation

[8] How a smart home can improve your home security, opt. cit.

[9] The strategic energy technology (SET) plan. In: *Op.europa.eu* [online]. Publications Office of the EU [cit. 24. 06. 2021]. p. 39. Available at: https://op.europa.eu/en/publication-detail/-/publication/064a025d-0703-11e8-b8f5-01aa75ed71a1

[10] COMMUNICATION FROM THE COMMISSION Towards an Integrated Strategic Energy Technology (SET) Plan: Accelerating the European Energy System Transformation. In: *Set-is.ec.europa.eu* [online]. Strategic Energy Technologies Information System. [cit. 08. 01. 2021]. p. 11.Available at: https://ec.europa.eu/energy/sites/ener/files/publication/Complete-A4-setplan.pdf

to reckon with the fact that a smart home won't bring you as many benefits as if you invested more in it. Thanks to energy savings, this investment pays off in the long run. [11] Another problem that a smart home can bring is, for example, when an overvoltage arises in connection with the interconnection of devices, which can cause demand, power outages or the case of mutual incompatibility between devices.[12]

However, one of the biggest pitfalls of smart homes is the fact that all smart home devices are connected to a common network. In addition to the traditional connection of computers to the network, in the household, we can also find, for example, the mentioned refrigerator, which is connected to other devices via one network. Connecting your smart home devices to a shared network can be a security threat to you. It is so important to monitor their security level when buying smart devices. Personal data that a smart device obtains from you can be misused by hackers. It is also important to keep in mind that these devices collect personal data about you, which can be used by various companies. By secretly monitoring your online activities, the company can target you with specific ads through a smart device.[13]

## 3. UNAUTHORIZED LEAKAGE OF PERSONAL DATA

Connecting your smart home devices to a shared network can be a security threat to you. Malicious actors could exploit device vulnerabilities or system errors to gain access to the entire home network to which the smart home is connected. [14] Poor security of smart appliances in a smart home can thus pose a real threat to household residents. The threat itself is that smart

[11] 30 Key Pros & Cons Of Smart Homes. In: *Environmental-conscience.com* [online]. 2020 [cit. 08. 01. 2021]. Available at: https://environmental-conscience.com/smart-homes-pros-cons/

[12] Ibid.

[13] SCHNEIER, Bruce. Essays: The Internet of Things That Talk About You Behind Your Back - Schneier on Security. In: *Schneier.com.* [online] *08.01.2016* [cit. 08. 01. 2021]. Available at: https://www.schneier.com/essays/archives/2016/01/the_internet_of_thin_1.html

[14] FERRON, Emily. 7 Tips to Protect Your Smart Home from Hackers. In: *Safety.com* [online]. 3. 6. 2019 [cit. 08. 01. 2021]. Available at: https://www.safety.com/how-to-protect-smart-home-from-hackers/

devices in a smart home can know virtually anything about their residents. They can monitor their activities, they know when they go to work, smart devices know their voices, their passwords and much more. These devices work with our personal data, which may fall into the wrong hands.

The most vulnerable devices include outdoor devices with a lower level of security. Examples are smart bells or an automatic garage door opener that can be easily accessed from the street, which hackers can exploit. [15] The level of security of these devices is therefore important. In November 2020, for example, Amazon UK's bestseller in smart doorbells was found to send unencrypted household names and passwords to servers in China. When purchasing these devices, the buyer should take into account the security risks and not prefer convenience. Consumers are then at high risk of their data being misused.[16]

Another vulnerable group are home devices that can be controlled via an application on your phone, tablet or home computer. These include security cameras, baby monitors, smart locks, personal home assistants and more. These can be easily compromised due to weaknesses in the communication protocol or vulnerable entry points that vendors have left accessible for subsequent maintenance.[17] In October 2016[18], a botnet known as "Mirai" infiltrated many connected devices to the Internet with the Linux operating system and turned them into a network of remotely controlled bots. He attacked mostly cameras connected to smart homes and personal home assistant devices. [19]

There are many known cases when hackers attack baby monitors. Initially, it may begin with a beep, and it may culminate in sexual exclamations, echoing through a baby monitor in the parents' room, which is con-

---

[15] Ibid.

[16] Smart doorbells „easy target for hackers" study finds - BBC News. In: *bbc.com.* [online]. 23.11.2020 [cit. 08. 01. 2021]. Available at: https://www.bbc.com/news/technology-55044568

[17] FERRON, Emily, opt. cit.

[18] CHEN, James. opt. cit.

[19] What is the Mirai Botnet?. In: *Cloudflare* [online] [cit. 08. 01. 2021]. Available at: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

nected to a camera in the children's room. Anxious parents who have heard the voice of a hacker through a baby monitor feel that someone is with their child. However, when they turn on the lights in the room, the hacker can tell them through the baby monitor to turn off the lights. The hacker can connect to other devices, incl. smart light bulbs in their smart home. However, when the child's parents come to the children's room, they find that there is no stranger in the room and find out that their smart home has been attacked by hackers. This really happened to the parents of a 4-month-old son on 17th December 2018, in Houston.[20]

Even hacking a robotic vacuum cleaner can be dangerous for households, for example, US experts have found that a robotic vacuum cleaner does not only have to collect dirt but can also collect personal data. Robotic vacuum cleaners can be hacked remotely so that they can also capture sound and eavesdrop on the occupants of the house. The robotic vacuum cleaner does not have to be fitted with a microphone. Remotely, hackers can eavesdrop on a robotic vacuum cleaner by accessing its "Lidar" reading. Lidar is a remote sensing technology for measuring distances. The emitted laser beam can be used to indicate sound vibrations acting on objects struck by the laser. Thus, hackers can practically eavesdrop on household members.[21]

Home appliances, such as refrigerators, stoves, or ovens, are less likely to be attacked, but can still be attacked by hackers. Hacking your smart refrigerator means much more to hackers than just finding out the contents of your refrigerator. This gives them access to your home network and allows them to find out all the information about you through it.[22] For example, hackers can exploit security vulnerabilities (e.g. this device does not valid-

[20] WANG, Amy B. Nest cam security breach: A hacker took over a baby monitor and broadcast threats, Houston parents say. In:*Washingtonpost.com* [online] 20.12.2018 [cit. 08.01.2021]. Available at: https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/

[21] CHADWICK, Jonathan. Researchers hack a robotic vacuum cleaner to record speech remotely. In: *Mail Online* [online]. 18. 11. 2020 [cit. 08.01.2021]. Available at: https://www.-dailymail.co.uk/sciencetech/article-8961729/Researchers-hack-robotic-vacuum-cleaner-record-speech-remotely.html

[22] FERRON, Emily, opt. cit.

ate security certificates) in access to the Gmail calendar used in the refrigerator and monitor activity for the user name and password.[23]

### 3.1 HOW TO PREVENT MY PERSONAL DATA FROM LEAKING?

So, the question remains, how can we prevent the security threats posed by a smart home? In this section, I will present some specific tips on how to minimize the risk of hacking. It should be noted that no network is 100% secure, only the potential risk of hacking can be reduced. The first step must be taken during the selection of the smart device. We have to ask ourselves, what do we really want our smart home to be able to do? Based on that, we decide which devices to buy. It is important to look mainly at the brand and quality of the smart device. A device that is too cheap and unreliable could pose a security threat. Another step is to create a suitable network for smart devices. You should have a quality Wi-Fi router with a verified brand and set a network name and password. It is also a good idea to hide the visibility of the network. Another option is to create a second network within the home with its own name and password only for smart home devices. The hacker would possibly only get into this network separate from the one where you have your sensitive information stored. [24]

It is important to have the devices updated because each update fixes some bugs that the device had. This will prevent hackers from infiltrating the device due to these bugs. Network vulnerabilities were detected, for example, in the Philips Hue smart light bulb, which consisted of a low-power wireless protocol. That's why Philips has released a new firmware update that changes it. It is thus obviously important to update your devices regularly. [25] It is also important to keep in mind that you should have a secure

---

[23] NEAGLE, Colin. Smart refrigerator hack exposes Gmail account credentials In: networkworld.com [online]. 26.08.2015 [cit. 19.06.2021]. Available at: https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

[24] FERRON, Emily, opt. cit.

[25] WINDER, Davey. How to stop your smart home spying on you. In: *the Guardian* [online]. 8. 3. 2020 [cit. 08.01.2021]. Available at: http://www.theguardian.com/technology/2020/mar/08/how-to-stop-your-smart-home-spying-on-you-lightbulbs-doorbell-ring-google-assistant-alexa-privacy.

and specific password for each device. For example, if you use one password for all your operations and a hacker can access it, it will not be a problem for him to access your home network and thus all personal information about you.[26] To maximize security, so-called two-factor authentication is suitable for access to smart devices. To access the account of these devices, a password and secondary verification will be required, which most often consists of sending an SMS code to a mobile phone. This means that even if a hacker obtains your password, he will not get into the device, because he also needs a code sent to the mobile phone. [27] It is also advisable to disconnect devices that will not be used from electricity if we are leaving home for a long time (e.g. go on holiday). On the one hand, it will save energy and at the same time prevents hackers from hacking into your home network via this device while you are away.[28]

## 4. CONCLUSION

Thanks to this work, I was able to find out that a smart home consists of connecting individual smart devices to a common network, where it is possible to centrally control the devices using a smartphone, tablet or other similar networked devices. This has a number of advantages, such as energy savings, comfort or the ability to control your home from virtually anywhere. On the other hand, there are a number of disadvantages, the most fundamental of which are the security risks associated with a smart home. It is the connection of devices to the common network that is a great risk, because if a hacker gets into this network by hacking one device, he/she can then control all other devices and collect the collected data from them. This is also part of the answer to my research question. There are different levels of threat that a given smart device will be hacked. E.g. the biggest security risks are smart entrance locks and the least common are smart home appliances such as a refrigerator. There are many ways to pre-

[26] FERRON, Emily. 7 Tips to Protect Your Smart Home from Hackers.

[27] COHEN, Jason. How to Protect Your Smart Home From Hackers. In: *PCMAG* [online] [cit. 08.01.2021]. Available at: https://www.pcmag.com/how-to/how-to-protect-your-smart-home-from-hackers

[28] FERRON, Emily. 7 Tips to Protect Your Smart Home from Hackers.

vent hackers from gaining access to a smart home network. This can be achieved by using a strong password, choosing a suitable smart device or creating a second network only for smart home devices. However, there are many more options. That was s the answer to the second part of my research question.

In this work, I present a comprehensive view of how the safety of the residents of a smart household can be endangered and how this risk can be avoided. In principle, it can be said that it depends on the security level of the smart home. The more secure a smart home is, the more we have it under control and thus there will be no unauthorized access of third parties to our sensitive information.

## 5. BIBLIOGRAPHY

[1] CHEN, James. Smart Home. In: *Investopedia* [online] [cit. 08.01.2020]. Available at: https://www.investopedia.com/terms/s/smart-home.asp

[2] What is a Smart Home? - Smart Home Energy. In: *Smarthomeenergy.co.uk* [online]. [cit. 08. 01. 2021]. Available at: http://smarthomeenergy.co.uk/what-smart-home

[3] All Samsung Family Hub Features | Samsung US. In: *Samsung Electronics America* [online] [cit. 08. 01. 2021]. Available at: https://www.samsung.com/us/explore/family-hub-refrigerator/apps/

[4] How a smart home can improve your home security. In: *Hestiamagazine.eu* [online]. 2021 Hestia Magazine [cit. 24. 06. 2021]. Available at: https://www.hestiamagazine.eu/how-a-smart-home-can-improve-your-home-security

[5] Greatest Advantages of Smart-Home Automation. In: *Bluespeedav.com* [online]. [cit. 08. 01. 2021]. Available at: https://bluespeedav.com/blog/item/7-greatest-advantages-of-smart-home-automation

[6] The strategic energy technology (SET) plan. In: *Op.europa.eu* [online]. Publications Office of the EU [cit. 24. 06. 2021]. p. 39. Available at: https://op.europa.eu/en/publication-detail/-/publication/064a025d-0703-11e8-b8f5-01aa75ed71a1

[7] Communications from the Commision Towards an Integrated Strategic Energy Technology (SET) Plan: Accelerating the European Energy System Transformation. In: *Setis.ec.europa.eu* [online]. Strategic Energy Technologies Information System. [cit. 08. 01. 2021]. Available at: https://ec.europa.eu/energy/sites/ener/files/publication/Complete-A4-setplan.pdf

[8] 30 Key Pros & Cons Of Smart Homes. In: *Environmental-conscience.com* [online]. 2020 [cit. 08. 01. 2021]. Available at: https://environmental-conscience.com/smart-homes-pros-cons/

[9] SCHNEIER, Bruce. Essays: The Internet of Things That Talk About You Behind Your Back - Schneier on Security. In: *Schneier.com.* [online]. 08.01.2016 [cit. 08. 01. 2021]. Available at: https://www.schneier.com/essays/archives/2016/01/the_internet_of_thin_1.html

[10] FERRON, Emily. 7 Tips to Protect Your Smart Home from Hackers. In: *Safety.com* [online]. 3. 6. 2019 [cit. 08. 01. 2021]. Available at: https://www.safety.com/how-to-protect-smart-home-from-hackers/

[11] What is the Mirai Botnet? In: *Cloudflare* [online] [cit. 08. 01. 2021]. Available at: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[12] WANG, Amy B. Nest cam security breach: A hacker took over a baby monitor and broadcast threats, Houston parents say In:*Washingtonpost.com* [online]. 20.12.2018 [cit. 08.01.2021]. Available at: https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/

[13] CHADWICK, Jonathan. Researchers hack a robotic vacuum cleaner to record speech remotely. In: *Mail Online* [online]. 18. 11. 2020 [cit. 08.01.2021]. Available at: https://www.-dailymail.co.uk/sciencetech/article-8961729/Researchers-hack-robotic-vacuum-cleaner-record-speech-remotely.html

[14] NEAGLE, Colin. Smart refrigerator hack exposes Gmail account credentials In: *networkworld.com* [online]. 26. 08. 2015 [cit. 19.06.2021]. Available at: https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

[15] WINDER, Davey. How to stop your smart home spying on you. In: *the Guardian* [online]. 8. 3. 2020 [cit. 08.01.2021]. Available at: http://www.theguardian.com/technology/2020/mar/08/how-to-stop-your-smart-home-spying-on-you-lightbulbs-doorbell-ring-google-assistant-alexa-privacy.

[16] COHEN, Jason. *How to Protect Your Smart Home From Hackers.* In: *PCMAG* [online]. [cit. 08.01.2021]. Available at: https://www.pcmag.com/how-to/how-to-protect-your-smart-home-from-hackers

# CHILLING EFFECT: HOW LACK OF PRIVACY AFFECTS THE POLITICAL FREEDOM AND SOCIAL DISSENT[1]

*JANA KRČMOVÁ*[2]

## 1. PRIVACY

Trying to clearly define what exactly privacy is seems like an impossible task. It has been described in a wide variety of ways, which is understandable, considering that the concept we are trying to put into words is both intangible and so subjective, so personal – it makes sense that each person's opinion on what privacy means to them would differ, sometimes very greatly. There is not much more consensus in academic spaces. In fact, one might say that one of the most common threads running through different descriptions of "privacy" would be that it is hard to describe. Complicated. Each concept is tinged with a variety of philosophical, sociological, or political theories.[3] However, its' importance – to us, as autonomous individuals, our development and wellbeing, to our relationships, and to the good of our society as a whole, is much less disputed.[4]

## 2. CHILLING EFFECT

Chilling effect was first articulated in express terms in the USA, during the Cold War, in connection to the First Amendment, which states that "*Congress shall make no law respecting an establishment of religion, or prohibiting*

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Surveillance. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Surveillance.

[2] Jana Krčmová je studentkou Právnické fakulty Masarykovy univerzity. Kontakt: 468555@mail.muni.cz.

[3] KOOPS, Bert-Jaap; NEWELL, Bryce Clayton; TIMAN, Tjerk; ŠKORVÁNEK, Ivan; CHOKREVSKI, Tom and Maša GALIČ. A Typology of Privacy. *University of Pennsylvania Journal of International Law 38(2): 483-575 (2017), Tilburg Law School Research Paper No. 09/2016*, pp. 491-492.

[4] NISSENBAUM, Helen. *Privacy in context: Technology, Policy, and the Integrity of Social Life*. Vol. 1. Stanford, California: Stanford University Press, 2010, pp. 81-88.

*the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."*[5] In reaction to the anti-communist government measures of the time, the courts came to the conclusion that certain acts of government "might deter the free exercise" of a person's rights, because of fear of prosecution. This theory functions similarly in online spaces – people might be deterred from engaging in (or might censor themselves while engaging in) certain legal activities online (such as discussions of matters of public interest and political issues, research into certain topics, which is not only legal but vital for the function of a democratic society) because of government surveillance of these online spaces, whether because they fear actual legal retribution or they fear being labelled as "someone to watch" (they fear that the general mass surveillance they are under will turn into personal surveillance, and all this would happen without their knowledge, making it impossible to gauge if and how closely is one being watched). However, research suggests that while people might express privacy concerns in connection to their online presence, this might not actually impact their behaviour in these spaces all that much.[6]

## 3. BEYOND NOTHING TO HIDE

In a 2017 study titled "*Beyond nothing to hide*" Stuart and Levine examined people's position on surveillance in today's online spaces. Through analysis of interviews conducted with the participants (there were 42 participants in total, aged 18-46, all students at a British university, but not all British nationals) in focus groups, the researchers were able to make several observations.

The subjects seemed to think of surveillance as quite ubiquitous but they were not particularly stirred to oppose this. In fact, the notion that they were already under surveillance in one way or other served as an argument

[5] Amend. I, U.S. Const. In: *CONSTITUTION ANNOTATED* [online]. CONGRESS.GOV [cit. 31. 11. 2020]. Available at: https://constitution.congress.gov/constitution/amendment-1/

[6] PENNEY, Jonathon W. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal.* 2016, Vol. 31, No. 1, pp. 125-129.

that more surveillance would not be a problem for them – as long as the way it was implemented was normal ("everyone does that") and had a legitimate goal, in improving services or providing more security. It would however be inaccurate to say that they were clearly in favour of further surveillance, or even the current state of it, but that they were resigned to it.[7] Surveillance seems to come attached with a sort of normalising effect. What would have seemed an unacceptable intrusion into a person's privacy to previous generations, we accept simply as a part of navigating the world, especially online. There is a sort of a trade-off, in which we allow some intrusion into our privacy for some sort of service.[8]

The next logical question then would be – when do we mind? In which circumstances do we find that the trade-off no longer benefits us?

Surveillance, with the use of technology, has a leg up on any more traditional sort of surveillance. It is integrated into our surroundings, in ways that make it feel inobtrusive, imperceptible, even convenient.[9] (To illustrate this point, an example from personal experience: recently I've turned off targeted ads on YouTube and then gotten legitimately annoyed at how off the mark most of the ads I had started to see were – an app store for a brand of a mobile phone which I do not have being the most often recurring one. A similar amount of car commercials though, which are as relevant to me, a 22-year-old student, as they were before when they were targeted.) That does not mean that surveillance is always perfectly seamless.

Such is the case when we consider the surveillance to be excessive – when the trade-off is mismatched. Even then, the responders either considered it to be harmless (the "nothing to hide" argument) or simply accepted it because of the necessity of the service provided (Google is necessary, therefore we have to give up privacy and place our trust in the provider of said service).[10] Secondly, the threat of future surveillance technology (discussed in the study in connection to Google Glass) – concerns that surveil-

[7] STUART, Avelie; LEVINE, Mark. Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *European Journal of Social Psychology*. 2017, Vol. 47, p. 698.

[8] Ibid., p. 704.

[9] Ibid., p. 705.

[10] Ibid., pp. 698-699.

lance will become even more present (capturing not just our activity on the internet, but our 'real' lives, more on this later) and harder to detect. However, the responders also note that this development does not sit well with them simply because they are not used to it – it has not yet been normalized.[11] Lastly, instances when surveillance seems to notice 'us'. When we feel we cannot keep parts of our lives to ourselves, parts of our identities separate or when there are real, unforeseen, and unwanted consequences or when we feel misrepresented.[12]

Throughout, Stuart and Levine refer to a different study, by Ellis, Harper, and Tucker, published in 2013, "The affective atmospheres of surveillance;" in which the respondents stated that they feel they are always being observed, but they found it difficult to even articulate this in any concrete terms, a situation which does not lend itself to much resistance.[13] The last point of discussion in "Beyond nothing" deals with exactly that – how respondents deal with surveillance and its' potential negative effects, which is through separation – understood as the ability to distance oneself from undesirable associations.

Separation of the physical person and the digital person, which makes the surveillance of the digital person inconsequential to them, the "real" person. Whether you are under surveillance on the internet has little to no impact on your actual life.[14]

However, what does seem to have an immediate effect, is peer-to-peer surveillance.

## 4. PEER-TO-PEER SURVEILLANCE AND THE EXTENDED CHILLING EFFECT

Helen Nissenbaum's theory of privacy as contextual integrity – that we are people who exist in various social contexts, which, in order for us to perform the variety of roles we inhabit in other people's lives, must remain

[11] Ibid., p. 700.

[12] Ibid., pp. 700-702.

[13] Ibid., pp. 696.

[14] Ibid., p. 702 and p. 704.

separate. We feel that our privacy is threatened when these context-relative informational norms are being disturbed.[15]

Through social networking sites we can interact with a vast variety of people, from absolute strangers through family members both close and distant to (potential or actual) employers and co-workers. We are also afforded an opportunity that is not so present in our 'real-world' lives, the opportunity of impression management. In short, we have much more control over the image we put out on the internet, but this image we choose to project is necessarily impacted by our audiences' expectations. As said above, we play a variety of roles in different social contexts (we act differently when we are with our friends than we do in front of our employers, in each situation we make different judgements of what is and what is not appropriate), but on social networking sites, our audience is mixed, and we have to present our online personas in a way that works for all of them, without appearing dishonest, and thus making our aim at the lowest common denominator, with the intention to alienate as few people as possible.[16]

The extended chilling effect then refers to the way online surveillance might affect our presentation offline – how our image online and offline match-up, how our actions in real life might be portrayed in online spaces and impact our image that way, and changing how we act in "real life" because of how it might appear if connected to us in an online space, through social networks.[17] Examples of this might range from the innocuous ("do not tag me in that photo, I look like I'm drunk in it") to the quite serious (pictures of political protests, in which individual protesters can be identified[18]).

---

[15] NISSENBAUM, Helen. *Privacy in context: Technology, Policy, and the Integrity of Social Life*. Vyd. 1. Stanford, California: Stanford University Press, 2010, p. 186.

[16] MARDER, Ben; JOINSON, Adam; SHANKAR, Avi; HOUGHTON, David. The extended 'chilling' effect of Facebook: The cold reality of ubiquitous social networking. *Computers in Human Behaviour*. 2016, Vol. 60, pp. 582-584.

[17] Ibid., pp. 584-589.

[18] SHEPHERD, Katie. An artist stopped posting protest photos online to shield activists from police. Then, he was arrested. *The Washington post* [online]. The Washington Post, published 3.8.2020 [cit. 1.11.2020]. Available at: https://www.washingtonpost.com/nation/2020/08/03/philadelphia-arrest-protest-photos/

## 5. A DIFFERENT PERSPECTIVE

So far, "Beyond nothing to hide" has been our reference point. But, as the authors themselves point out, their subject pool was quite limited (with the respondents all being students, mostly young adults and all heavily involved with social media, while not engaging in much that might be seen as sensitive, politically – people that have "nothing to hide") – responses would likely be quite different if the people questioned were part of, for example, "stigmatised minority".[19] Such being the case, we might want to explore the chilling effect in different sorts of circumstances.

There was a noticeable shift in the wake of the Snowden leaks in how we think of surveillance. It brought certain issues to the forefront of the minds of the wider public. Previously covert surveillance was no longer so. In the aftermath of this incident, Jonathan W. Penney examined the influence of chilling effect on what might seem like quite an inoffensive activity – reading articles on Wikipedia. In particular, he examined the effect the Snowden leaks (an "exogenous shock") had on Wikipedia traffic for articles on privacy-sensitive topics, with keywords such as "Car bomb", "Homeland defence" or "Liberation Front" to pick a few at random, and did, in fact, find that there was a quite significant drop in traffic, and so was able to conclude that chilling effect had an impact on this entirely legal and in fact quite necessary activity (the public educating itself on sensitive topics).[20]

There are far more blatant examples of chilling effect to be found in the world – with Mainland China being an obvious place to look. In some ways, there is not even a lot of space for self-censure to apply – instead of being monitored, the access to quite a few websites is simply blocked, even before Xi Jinping's "Great Firewall of China", which heavily solidified these restrictions, with Chinese online space truly becoming a world onto itself.[21] But if we are to provide just one example, to tie in with the previously mentioned notion that the situation would be different if the respondents

[19] STUART, Avelie; LEVINE, Mark. Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *European Journal of Social Psychology*. 2017, Vol. 47, p. 704

[20] PENNEY, Jonathon W. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal.* 2016, Vol. 31, No. 1, pp. 119-125, 159-161 and pp. 177-182.

were of a "stigmatised minority", we should not look any further than the situation of Uighur Muslims: of particular note to this topic being the language used by the people targeted (for example, disappeared people described as having "gone back home").[22]

## 6. CONCLUSION

Most of us (if by 'us' we mean the average user of social media in a democratic country) do not walk around constantly chilled by fear of what our everyday internet activity might mean for us, because there usually are not any actual consequences attached, imagined or real. Nevertheless, that does not mean we have to agree with the surveillance. It might make us uncomfortable, or "creeped out". We might be constrained by the expectations of our peers. We might oppose the scope of surveillance levelled at us, or the way already obtained data is handled. We might oppose having our privacy be at the whims of the free market (and we might even be right to do so),[23] but none of these really makes the chill, as it was first defined, set in – that comes with consequences. Neither the government nor the private companies that have access to our data care how often we listen to Britney Spears' hit song 'Toxic' at four a.m. Now, that might change – if Britney Spears were to poison the president of the U.S.A., the public opinion on her song would, most likely, shift – and while it still would not be (hopefully) illegal to listen to 'Toxic', the connotations around it would adjust – in response to an exogenous shock.

To conclude, aside from the notion that there maybe should be widerspread awareness of one's rights on the internet – privacy is valuable. For

[21] ECONOMY, Elizabeth C. The great firewall of China: Xi Jinping's internet shutdown. *The Guardian* [online]. Guardian News & Media Limited, published 29.6.2018 [cit. 1.11.2020]. Available at: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

[22] BUNIN, Gene A. 'We're a people destroyed': why Uighur Muslims across China are living in fear. *The Guardian* [online]. Guardian News & Media Limited, published 7.8.2018 [cit. 1.11.2020]. Available at: https://www.theguardian.com/news/2018/aug/07/why-uighur-muslims-across-china-are-living-in-fear

[23] NISSENBAUM, Helen. *Privacy in context: Technology, Policy, and the Integrity of Social Life*. Vol. 1. Stanford, California: Stanford University Press, 2010, p.87.

us, as individual people, for our mental and social wellbeing, but it is also valuable for society, both as a collection of individuals, in which case it is certainly better that this collection of individuals was not made unwell by the strain of surveillance, and as a space in which we all come together, where we can (attempt to) come to a consensus, based on our personal experiences and our opinions, which we were able to form freely, without fear of persecution.

## 7. BIBLIOGRAPHY

[1] BUNIN, Gene A. 'We're a people destroyed': why Uighur Muslims across China are living in fear. *The Guardian* [online]. Guardian News & Media Limited, published 7.8.2018 [cit. 1.11.2020]. Available at: https://www.theguardian.com/news/2018/aug/07/why-uighur-muslims-across-china-are-living-in-fear

[2] ECONOMY, Elizabeth C. The great firewall of China: Xi Jinping's internet shutdown. *The Guardian* [online]. Guardian News & Media Limited, published 29.6.2018 [cit. 1.11.2020]. Available at: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

[3] KOOPS, Bert-Jaap; NEWELL, Bryce Clayton; TIMAN, Tjerk; ŠKORVÁNEK, Ivan; CHOKREVSKI, Tom and Maša GALIČ. A Typology of Privacy. *University of Pennsylvania Journal of International Law 38(2): 483-575 (2017), Tilburg Law School Research Paper No. 09/2016*.

[4] MARDER, Ben; JOINSON, Adam; SHANKAR, Avi; HOUGHTON, David. The extended 'chilling' effect of Facebook: The cold reality of ubiquitous social networking. *Computers in Human Behaviour*. 2016, Vol. 60.

[5] NISSENBAUM, Helen. *Privacy in context: Technology, Policy, and the Integrity of Social Life*. No. 1. Stanford, California: Stanford University Press, 2010.

[6] PENNEY, Jonathon W. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal.* 2016, Vol. 31.

[7] SHEPHERD, Katie. An artist stopped posting protest photos online to shield activists from police. Then, he was arrested. *The Washington Post* [online]. The Washington Post, published 3.8.2020 [cit. 1.11.2020]. Available at: https://www.washingtonpost.com/nation/2020/08/03/philadelphia-arrest-protest-photos/

[8] STUART, Avelie; LEVINE, Mark. Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *European Journal of Social Psychology*. 2017, Vol. 47.

[9] Amend. I, U.S. Const. In: *CONSTITUTION ANNOTATED* [online]. CONGRESS.GOV [cit. 31. 11. 2020]. Available at: https://constitution.congress.gov/constitution/amendment-1/

# FREEDOM OF SPEECH VS. RIGHT TO BE FORGOTTEN: A COMPARISON OF EUROPEAN AND US PERSPECTIVE[1]

*JANA KRČMOVÁ*[2]

## 1. INTRODUCTION

One of the things that might be safe to say is that every internet user has heard 'Once you put it out on the internet, it'll be there forever!' or some variation thereof. It is a bit of a cliché. After all, we lose track of things on the internet all the time: servers shut down, once popular sites close, or an unexpected 'update' wipes everything you put there clean. But as children gain unrestricted access to the internet at an increasingly young age, often without much education to the tune of "Never give any of your personal information to anyone" and "Literally everyone on the internet, aside from yourself, is a 50 year old man just pretending to be a 12 year old girl" that older generations received (which, it has to be said, were quite a bit exaggerated, but they did their job of making people at least a little bit more cautious then they would have been otherwise).[3] Internet's memory, technological memory, does not function the way human memory does, it does not forget at the same rate or the same way – if it forgets at all. Embarrassing or ill-considered things once would have remained only in our parents' photo albums or our friends' stories, contained in a relatively small social circle. Even the most vicious gossip would not have much reach (if you were not already widely known, of course) and would disappear over time. Our personal data, freely floating across the internet (or downloaded or

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Rights of the data subject, Duties of the data controller. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Rights of the data subject, Duties of the data controller.

[2] Jana Krčmová je studentkou Právnické fakulty Masarykovy univerzity. Kontakt: 468555@mail.muni.cz.

[3] GREEN, Alex; WILKINS, Clare; WYLD, Grace; MANNING, Cliff. Keeping childern safe online. In: *London: New Philantrophy Capital.* [online] 2019, p. 32 [cit. 5. 12. 2020]. Available at: https://www.thinknpc.org/resource-hub/keeping-children-safe-online/

screenshotted etc.) for the rest of eternity is a daunting prospect.[4] In response to this, the right to be forgotten might come to mind. But what exactly is it? How does it work? And how does the right to free speech intersect with it?

## 2. FREEDOM OF SPEECH

### 2.1 EUROPEAN PERSPECTIVE (COUNCIL OF EUROPE/EU)

Under the European Convention on Human Rights, the protection of the freedom of expression can be found in Article 10, and includes "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers".[5] Variations thereof can be found in written constitutions and bills of rights all across the globe – for example, it is expressed quite similarly in Article 11 of the Charter of Fundamental Rights of the European Union.[6] As is expressly stated in the European convention, this right protects the speaker as well as the listener. It protects not only the information itself but also the channels through which it is transmitted because the interference with means of transmission would doubtless impact the freedom of speech itself. The internet is currently an important conduit for the spread of information, whether in the hands of the traditional press, governmental or other organizations, or regular users, as the European Court of Human Rights states that 'user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression.'[7]

The importance of its protection is inarguable, on its own and in its' importance for the protection of other rights. It is vital for the basic function-

[4] POLITOU, Eugenia; ALEPIS, Efthimios; PATSAKIS, Constantinos. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity* [online]. 2018, pp. 2-4 [cit. 5. 12. 2020]. Available at: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056

[5] Article 10 of European Convention for the Protection of Human Rights and Fundamental Freedoms, amended version. In: *European Court of Human Rights* [online]. Council of Europe [cit. 5. 12. 2020]. Available at: https://echr.coe.int/Documents/Convention_ENG.pdf

[6] Article 11 Charter of Fundamental Rights of the European Union, 12.12.2007. In: EUR-Lex [online]. Úřad pro publikace Evropské unie [cit. 5. 12. 2020]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

ing of democracy, and the personal development of every human being. This however does not mean that it is absolute and can never be restricted. On the contrary, freedom of expression clashes with other rights quite often: with the right to a fair trial, to conscience and religion, but that right to free speech seems to be in the best position to challenge is the right to privacy and the rights related to it – respect for private life, data protection, right to be forgotten etc., because, in some areas, they seem to directly oppose each other. But as with any conflict of protected rights, the balance must be struck according to each situation – no one right takes precedent automatically. The second paragraph of Article 10 of ECHR itself expresses that since the right "carries with it duties and responsibilities", it may be subject to restrictions.[8] Some forms of speech are always outside the protection provided by Article 10: hate speech, incitement to violence, holocaust denial and speech promoting the Nazi ideology.[9] Aside from this, the Court uses a three stage test to judge whether state interference is permissible: it has to be prescribed by law, pursue a legitimate aim, and be necessary for a democratic society.[10] Restriction of free speech in the Charter of Fundamental Rights of the EU functions similarly, as set forth in Article 52 paragraph 1. In paragraph 3, the Charter expressly states that 'the meaning and scope of those rights shall be the same as those laid down by the said Convention,' referring to the ECHR.[11]

---

[7] KULK, Stefan; ZUIDERVEEN BORGESIUS, Frederik. Privacy, freedom of expression, and the right to be forgotten in Europe. *Cambridge Handbook of Consumer Privacy* [online]. 2018, pp. 6-7 [cit. 5. 12. 2020]. Available at: https://www.researchgate.net/publication/320456033_Privacy_freedom_of_expression_and_the_right_to_be_forgotten_in_Europe

[8] BYCHAWSKA-SINIARSKA, Dominika. Protecting the Right to Freedom of Expression under the European Convention on Human Rights. A Handbook for Legal Practitioners. Council of Europe. 2017, p. 11-12. Available at: https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814

[9] BYCHAWSKA-SINIARSKA, op. cit., pp. 23-30.

[10] BYCHAWSKA-SINIARSKA, op. cit., pp. 32-33.

[11] EU Charter, Article 52.

## 2.2 US PERSPECTIVE

In the United States, protection of freedom of speech is guaranteed in the Bill of Rights, as the First Amendment states that "Congress shall make no law … abridging the freedom of speech, or of the press"'.[12] Though originating in the 18th century and thus preceding the original version of the European convention by nearly 200 years, its' intentions do not much differ, even if they are expressed considerably more succinctly. As Thomas I. Emerson writes, the necessity of functions of the First Amendment, for a liberal constitutional state, can be placed under four categories: individual self-fulfilment, means of attaining the truth, method of securing participation by the members of the society, including political, decision-making and lastly maintaining the balance between stability and change in society. Although articulated in 1961, these categories still ring true, but as he also states, the right to freedom of expression is not a new concept, and has changed before and must again, in response to different conditions and current problems.[13] Even as far as the late nineteenth century, in Warren's and Brandeis' "The right to privacy", concerns regarding the scope of the First Amendment with regards to the development of technology can be found.[14]

Unlike the ECHR, there is no provision to be found in the Bill of Rights concerning the limits of free speech – for that, we must look elsewhere, particularly to judicial decisions of the Supreme Court of the United States. Regarding specifically the issue of privacy, several important cases should be mentioned. In Cox Broadcasting Corp v. Cohn, the Supreme Court has ruled that a newspaper publishing company (Cox) could not be held liable for the dissemination of publicly available information (name of a deceased rape victim), basing this decision on public interest. In Smith v. Daily Mail Publishing, the newspaper was not found liable for the publication of the name of a juvenile murder suspect (obtained this time not from records

[12] Amend. I, U.S. Const. In: *CONSTITUTION ANNOTATED* [online]. CONGRESS.GOV [cit. 5. 12. 2020]. Available at: https://constitution.congress.gov/constitution/amendment-1/

[13] EMERSON, Thomas I. Toward general theory of the first amendment. *Yale Law Journal.* 1963, vol. 72, no. 5, p. 878.

[14] WARREN, Samuel D., and Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review*. 1890, vol. IV, pp. 193–220.

kept by the state, but by interviewing witnesses), the Supreme Court stated that an infringement on the freedom of the press would only be permissible if necessary to advance a state interest of "the highest order". A similar decision to Cox was reached in The Florida Star v. B.J.F., in which another victim of a sexual offence sought redress for the damage caused by her full name being published in connection to an ongoing case, with the perpetrator still at large, which led to her being harassed. The Supreme Court, citing public interest 'in the investigation of a violent crime', ruled in favour of the defendant. The definition of 'of public interest' in Supreme Court doctrine seems rather wide, covering a broad range, including dissemination of the sort of information that hardly seems actually relevant to the public – surely the public can be informed without putting the victim at risk.[15] Emerson in his article comments on the "unsatisfactory state" of the doctrine surrounding the first amendment, calling proponents of "absolute" interpretation of the Amendment impractical and proponents of balancing tests reductionist.[16] Leslie Kendrick, in her much more recent writing, criticises what she calls First Amendment opportunism and First Amendment expansionism and the abundance of different theories of application that surround it.[17]

## 3. RIGHT TO BE FORGOTTEN

### 3.1 EUROPEAN PERSPECTIVE (EU)

The right to be forgotten can be found in EU Regulation 2016/679, General Data Protection Regulation or as it is commonly known, the GDPR, as the right to erasure, with "right to be forgotten" in brackets. It allows for a subject to request the erasure of their personal data by the data controller, with the data controller being obliged to do so without further delay if one

[15] WERRO, Franz. The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash. *Liability in the Third Millenium*. 2009, pp. 293-297.

[16] EMERSON, op. cit., p. 877.

[17] KENDRICK, Leslie, First Amendment Expansionism. *56 WM. & MARY L. REV. 1199*. 2015, vol. 56, no. 4, pp. 1199-1220.

of the outlined conditions applies.[18] This version of the right to be forgotten is a considerable step back from the originally proposed version, which was widely criticised, with one of its' loudest critics being Peter Fleischer, chief privacy counsel of Google at the time, who outlined three categories of personal data that the proposed version covered, with each category being a greater threat to free speech than the one before it. The first category covers information that a person puts online themselves – in this category, being able to delete our own content is the norm and making this enforceable would be largely symbolic. The second covers content that people also posted themselves, which was then copied and posted by other users, which is more of a challenge to freedom of speech. The third category contains information posted about a person by a third party, which could also be deleted upon request if certain conditions were met. This would, Rosen argues, produce a chilling effect, leading data controllers to delete as requested even in ambiguous cases.[19] Although these arguments were made in regard to a never passed version of the right in question, similar suspicions follow the GDPR version as well, which is admittedly still a breakthrough, if not quite revolutionary. It draws from the concept of individuals' right to data self-determination and legislation of several European countries that include some sort of right to be forgotten, which usually pertains to individuals' criminal past, such as France's Right to Oblivion or Swiss 'die Persönlichkeitsrechte' (rights of the personality, which also include the right to be forgotten). Of particular interest is the ability of an individual to request the erasure of their data from every data controller, not only the first one, which aside from questions of law brings with it many technological challenges. As mentioned above, RtbF is surrounded by quite a bit of controversy, with solid arguments both for and against. There have been arguments for it as a human right, an expression of the broader right to

[18] Article 17 Regulation of the European Parliament and of the Council 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In: EUR-Lex [online]. Publications Office of the EU [cit. 6. 12. 2020]. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=en

[19] ROSEN, Jeffrey. The Right to be Forgotten. *Stanford Law Review Online.* 2011/2012, vol. 64, pp. 88-92.

privacy, arguments for it as a right to identity, as an expression of a person's right to change themselves, or simply as a psychological necessity. It has been proposed that the RtbF is not intended as a tool or erasure but as more human sort of forgetting, which would allow some leeway in its' implementation. Its' opponents, as might be expected, argue against it as being unprecedently dangerous to the freedom of expression, as a tool of censorship, or as Rosen, warning of a possible chilling effect, or destroying the impartiality of search engines.[20]

### 3.2 US PERSPECTIVE

One of the things that all three cases listed under the section 'USA perspective' on freedom of speech have in common is that they concerned a clash between state legislation and a constitutionally protected right. That is the crux of the problem – while freedom of speech is guaranteed by the Bill of Rights, on the federal level, privacy rights in the USA are provided for primarily by the Privacy act of 1974, which does not account for current issues in privacy law. There have been attempts at change, particularly in the last decade, (the Consumer Privacy Bill of Rights in 2015, for example) but none have (so far) been successful.[21] As written above, the First Amendment has exhibited a tendency to stretch. As such, it seems that the RtbF is fundamentally at odds with the First Amendment and the theory surrounding it. This idea is expressed, for example, by R. G. Larson III, who argues that it would restrict people's decisions with regards to what they say and think, undermine the normal function of communication, limit "the degree to which people may participate in the marketplace of ideas", and, lastly but perhaps most importantly, 'grant the legislature a power best left to the people.'[22] Werro, on the other hand, argues that this position stems

[20] POLITOU et al., op. cit., pp. 11-12.

[21] SHARK, Alan. Is it time for a national Digital Bill of Rights? *FCW post* [online]. 1105 Media, Inc., published 28.1.2020 [cit. 6.12.2020]. Available at: https://fcw.com/articles/2020/01/28/comment-data-privacy-bill-of-rights-shark.aspx

[22] LARSON III, Robert G. Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech. *Communication Law and Policy*. [online]. 2013, vol. 18, no. 1, pp. 119-120 [cit. 5. 12. 2020]. Available at: https://doi.org/10.1080/10811680.2013.746140

from American distrust of centralised power and faith in the private sector and the power of the free market and free press.[23]

## 4. CONCLUSION

The right to be forgotten (the right to privacy in general) and freedom of speech are often put into too sharp an opposition, which is not necessary. Both rights, the right to privacy and the right to expression are vital to our freedom. We cannot give up privacy in pursuit of freedom of expression because privacy is necessary for the function of freedom of speech, and on the flip side, freedom of speech allows us to express opinions that were allowed to develop in privacy. Knowing that every ill-considered, ill-informed, foolish, misguided, or simply embarrassing thing we ever let loose on the internet is going to stay around forever is clearly not conducive to the freedom of expression, is it? Would that knowledge not cause a person to monitor much more closely what they share, constantly on the lookout for any even potentially incendiary expression of their opinions? Would this not lead to (self) censorship? Be the cause of the chilling effect?[24] An example: Jon Ronson in 'So you've been publicly shamed' describes a case of a woman who became the subject of a widely spread harassment campaign after posting a certain picture in which she was making a rude gesture in front of a monument for veterans. In particular, the book describes a process that a certain company uses to make the internet 'forget' certain information, which they accomplish by putting out great amounts of information about the person, which pushes the content the person wants to be hidden to the second page of Google search results (which might as well be the Deep Web). The content they put out is purposefully deeply bland – what shows she likes, what animals, all in the pursuit of erasing the internet's memory of the picture (which was meant as nothing more than an inside joke), which led to her being extensively harassed and to her losing her job.[25] This

[23] WERRO, op. cit., p. 299.

[24] POLITOU et al., op. cit., p. 12.

[25] RONSON, Jon. *So you've been publicly shamed.* 1st edition. London: Pan MacMillan, 2015, p. 321. ISBN 1594487138.

is surely not free speech in action, as intended. Now, this is not a call for the RtbF to function unchecked. Its' use must be considered in each case's specific circumstances (nature of the information, the person's status, the time passed). But perhaps we can reconsider our perspective on the issue – with these two rights not as opposites of each other, but as each being necessary for the function of the other.

## 5. BIBLIOGRAPHY

[1] GREEN, Alex; WILKINS, Clare; WYLD, Grace; MANNING, Cliff. *Keeping childern safe online* [online]. London: New Philantrophy Capital. 2019, [cit. 5. 12. 2020]. Available at: https://www.thinknpc.org/resource-hub/keeping-children-safe-online/

[2] POLITOU, Eugenia; ALEPIS, Efthimios; PATSAKIS, Constantinos. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity* [online]. 2018 [cit. 5. 12. 2020]. Available at: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056

[3] European Convention for the Protection of Human Rights and Fundamental Freedoms, amended version. In: *European Court of Human Rights* [právní informační systém]. Council of Europe [cit. 5. 12. 2020]. Available at: https://echr.coe.int/Documents/Convention_ENG.pdf

[4] Charter of Fundamental Rights of the European Union, 12.12.2007. In: EUR-Lex [online]. Publications office of the EU [cit. 5. 12. 2020]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

[5] KULK, Stefan; ZUIDERVEEN BORGESIUS, Frederik. Privacy, freedom of expression, and the right to be forgotten in Europe. *Cambridge Handbook of Consumer Privacy* [online]. 2018, [cit. 5. 12. 2020]. Available at: https://www.researchgate.net/publication/320456033_Privacy_freedom_of_expression_and_the_right_to_be_forgotten_in_Europe

[6] BYCHAWSKA-SINIARSKA, Dominika. Protecting the Right to Freedom of Expression under the European Convention on Human Rights. A Handbook for Legal Practitioners. Council of Europe. 2017, Available at: https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814

[7] Amend. I, U.S. Const. In: *CONSTITUTION ANNOTATED* [online]. CONGRESS.GOV [cit. 5. 12. 2020]. Available at: https://constitution.congress.gov/constitution/amendment-1/

[8] EMERSON, Thomas I. Toward general theory of the first amendment. *Yale Law Journal.* 1963, vol. 72, no. 5.

[9] WARREN, Samuel D., and Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review*. 1890, vol. IV, s. 193–220.

[10] WERRO, Franz. The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash. *Liability in the Third Millenium*. 2009.

[11] KENDRICK, Leslie, First Amendment Expansionism. *56 WM. & MARY L. REV. 1199*. 2015, vol. 56, no. 4.

[12] Regulation of the European Parliament and of the Council 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In: EUR-Lex [online]. Úřad pro publikace Evropské unie [cit. 6. 12. 2020]. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=en

[13] ROSEN, Jeffrey. The Right to be Forgotten. *Stanford Law Review Online.* 2011/2012, vol. 64.

[14] RONSON, Jon. *So you've been publicly shamed.* 1st edition. London: Pan MacMillan, 2015, ISBN 1594487138.

---



---

# EU-UK DATA FLOWS IN POST-BREXIT TIMES[1]

*KAREL PELIKÁN*[2]

## 1. INTRODUCTION

We live in a highly globalized and connected world. Thus, in today's world, everybody relies on cross-border data flows, even the economy is built upon the free transfer of data. Expressed in numbers in 2014 data flows were worth $2.8 trillion of global GDP.[3] *"Globalization is a fact because of technology, because of an integrated global supply chain, because of changes in transportation, and we're not going to be able to build a wall around that,"*[4] Although I highly agree with the quote from the former United States (US) president Barack Obama, there is one wall that needs to be erected. The wall that is protecting the personal data flow. In my essay I will partly cover this topic, especially I will try to describe how Brexit will affect personal data flows between the United Kingdom (UK) and Europe.

## 2. PRE-BREXIT TIMES

For a better overview, I will shortly describe how the personal data flow between the UK and Europe looked like before Brexit. The UK's two first applications to join the EU in 1961 and 1963 were vetoed by the French. Finally, on 1 January 1973, the UK joined European Economic Community

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Trans-border data flow. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Trans-border data flow.

[2] Karel Pelikán je studentem Právnické fakulty Masarykovy univerzity. Kontakt: 483377@mail.muni.cz.

[3] Cross-border data flow [online]. In: *bsa.org* [cit. 8. 1. 2021]. Available at: https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf.

[4] HELLMAN, Jessie. Obama: We can't 'build a wall' around globalization [online]. In: *The Hill.* 22. 7. 2016. [cit. 8. 1. 2021]. Available at: https://thehill.com/blogs/ballot-box/presidential-races/288887-obama-slams-trump-trade-ideas-we-cant-build-a-wall-around.

(now the European Union - EU).[5] A major change in the EU-UK relationship was the UK's EU membership referendum held on 23 June 2016, where most votes were for the option of leaving the EU. That triggered Article 50 of the Treaty of Lisbon and started the two-year period of the UK formally leaving the EU also called Brexit. It was expected that the UK will leave the EU on 29 March 2019, but due to the problems on UK's side extensions were granted by European Council, hence the UK finally on 31 January 2020 left the EU.[6]

Until 31 January 2020 UK was still a member state of the EU, hence the personal data flow was regulated primarily by the EU legislation. For the purpose of this essay, I will not cover the EU legislation on personal data before the General Data Protection Regulation (GDPR). The regulation was adopted in 2016 by the EU and was put into effect on May 25, 2018.[7] One of the purposes of the GDPR was to achieve a free flow of personal data within the EU internal market: *the proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.*[8] Thus GDPR allowed a free personal data flow within the European Economic Area (EEA), which includes EU member countries and non-EU member countries such as Iceland, Liechtenstein, and Norway.[9] The above mentioned meant that there was free movement of personal data between the UK and the rest of EEA.

---

[5] When did Britain decide to join the European Union? [online]. In: *ukandeu.ac.uk*. 21. 8. 2020. [cit. 8. 1. 2021]. Available at: https://ukandeu.ac.uk/the-facts/when-did-britain-decide-to-join-the-european-union/.

[6] WALKER, Nigel. Brexit timeline: events leading to the UK's exit from the European Union [online]. In: *House of Commons Library*. 6. 1. 2021. [cit. 8. 1. 2021]. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-7960/.

[7] The History of the General Data Protection Regulation [online]. In: *edps.europa.eu* [cit. 8. 1. 2021]. Available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[8] Regulation of the European Parliament and of the Council (EU) 2016/679 of 18 April 2018 on on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[9] International transfers of personal data [online]. In: *European Commission* [cit. 8. 1. 2021]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en.

## 3. POST-BREXIT TIMES

After January 31, 2020 - the date the UK formally left the EU started a transition period. The transition period was set up in the revised Withdrawal Agreement that was agreed by the UK and EU in October 2019. This period spanned from January 31, 2020, until December 31, 2020. During this transition period, the GDPR continued to be applied in the UK. The UK National data protection authority - Information Commissioner's Office (ICO) stated that in the transition period it will not be necessary for organizations dealing with personal data to take immediate action such as additional safeguards.[10] Although the UK was not a member of the EEA, it has been treated as an EEA member during the transition period. That resulted in the free movement of personal data between the EEA and the UK in the transition period.[11]

Negotiations between the UK and the EU on future cooperation after Brexit in the transition period were tough and they took nine months. There was even a possibility of a hard Brexit, which would mean a no cooperation and trade agreement scenario. Finally, on 24. 12. 2020 the UK and the EU reached a comprise that lead to EU-UK Trade and Cooperation Agreement. The agreement is enormously huge it has more than 1000 pages and it covers areas such as fishing, dispute resolution, financial services etc. Most importantly for this essay, it somehow also covers the topic of data protection and data flow.[12] How is the EU-UK Trade and Cooperation Agreement going to affect the personal data flows between the UK and EEA? According to the agreement for the interim period of four to six months that started from 1 January 2021 the UK would not be treated as a third country. The benefits of not treating the UK as a third country in the

[10] SLINN, Benjamin., DE FONSEKA, Joanna. *Data Protection and Brexit* [online]. In: *Baker McKenzie* [cit. 8. 1. 2021]. Available at: https://www.bakermckenzie.com/-/media/files/insight/publications/2019/12/data-protection-and-brexit.pdf.

[11] MITCHELL, Ewen., SCHENKER, Sarah. C., Brexit: The Future of Data Flow to and from the EEA and the UK [online]. In: *GT London Law Blog*. 23. 12. 2020. [cit. 8. 1. 2021]. Available at: https://www.gtlaw-londonlawblog.com/2020/12/brexit-the-future-of-data-flow-to-and-from-the-eea-and-the-uk/.

[12] MORRIS, Chris. Brexit deal: What is in it? [online]. In: *BBC News.* 28. 12. 2020. [cit. 8. 1. 2021]. Available at: https://www.bbc.com/news/55252388.

interim period is that it is not necessary to have an adequacy decision for the UK or the organisations within the UK are not obligated to take a special safeguard based on article 46 of GDPR such as adequacy decisions, standard contractual clauses (SCC), binding corporate rules (BRC), certification mechanisms, codes of conduct, or so-called derogations. Another benefit is that this period gives the European Commission (EC) at least some time to finalise the adequacy decisions for the UK. The interim period will last for four months, but it can be extended to six months unless the UK or the EU will not raise an objection against the extension. There are two main conditions with which the UK must comply with. Firstly, UK is not allowed to change its legislation regarding data protection in the interim period. Secondly, the ICO cannot approve the transfer mechanisms or codes of conduct without permission from the EU-UK Partnership Council. The EU-UK Partnership Council is a body that oversees the EU-UK Trade and Cooperation Agreement and makes a recommendation regarding the functionality of the agreement. Furthermore, after the interim period, the UK is entitled to make changes in the data protection legislation in compliance with the fundamental principles of the GDPR and wider provisions of the EU-UK Trade and Cooperation Agreement. In the agreement, we can also find some commitments concerning personal data. For example, protection of the individuals from unsolicited direct marketing communications, sharing of passenger name records and vehicle registration information in the context of international travels or cooperation in the field related to criminal record information and DNA. Also, in the agreement, we can find the commitment to not restrict cross-border data flows for example by requiring data localisation. This will be under review and it will be evaluated within three years.[13]

From the above mentioned we know that in four or the maximum of six months the interim period will end and according to the GDPR the UK will be treated as a third country, thus according to the GDPR, a mechanism to

[13] BUNDY-CLARKE, Fiona. EU-UK Trade and Cooperation Agreement: Implications for data protection law [online]. In: *Data Protection Report*. 4. 1. 2021. [cit. 9. 1. 2021]. Available at: https://www.dataprotectionreport.com/2021/01/eu-uk-trade-and-cooperation-agreement-implications-for-data-protection-law/.

transfer data to third countries will be needed. As I mentioned above the GDPR offers a variety of mechanisms to transfer data to third countries.[14] The EC and the UK have decided to choose the adequacy decision. Based on article 45 of the GDPR: "*A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.*"[15] The adequacy decision is a multi-step process that includes a proposal from the EC, then also an opinion of the European Data Protection Board (EDB). There is also a need for approval from representatives of EU countries and finally, the decision must be adopted by EC. European Parliament (EP) and the European Council can request the EC to maintain, withdraw or amend the adequacy decision on the basis that its act exceeds implementing powers granted by GDPR. The adequacy decision allows the free movement of personal data from the EEA to a third country without any further safeguards.[16]

Is the adequacy decision an appropriate mechanism to transfer personal data to the UK? There is a certain level of uncertainty that arises from the Court of Justice of the European Union (CJEU) judgment in the Schrems II case. The case concerns the adequacy decision so-called the EU-US Data Protection Shield that enabled free movement of personal data from EEA to the US for organisations that were involved in it.[17] "*In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data*

[14] The EU Court of Justice invalidates EU-US Privacy Shield [online]. In: *dataprivacymanager-.net.* 21. 7. 2020. [cit. 9. 1. 2021]. Available at: https://dataprivacymanager.net/the-eu-court-of-justice-invalidates-eu-us-privacy-shield/.

[15] Article 45 of the regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[16] Adequacy decisions [online]. European Commission. [cit. 9. 1. 2021]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[17] The CJEU judgment of 16th July 2020, C-311/18, Schrems II.

*transferred from the European Union to that third country, which the Commission assessed in Decision 2016/1250, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary."*[18] This ruling set a high standard for adequacy decisions. It means that the level of protection must be essentially equivalent to that guaranteed within the EU by the GDPR. Based on this ruling the EU-US Data Protection Shield was invalidated.[19] The above mentioned could be a problem for the future adequacy decision for the UK because the current UK's security laws on data transfers are similar to the US ones and they grant UK's secret services quite invasive intelligence gathering powers. The US's security laws on data transfers and very powerful secrets services in term of intelligence gathering of personal data transfers were the key reasons why the EU-US Data Protection Shield was invalidated. Furthermore, according to the UK's national digital strategy, the government of the UK is planning to narrow some parts of its version of the GDPR.[20] The UK government stands before a tough decision. If they want to have an adequacy decision that would be the best data transfer mechanism from a business point of view, they will need to probably change their security laws on data transfers based on the Schrems II case.

To be precise the adequacy decision is not the only transfer mechanism to third countries, but it is the only one that does not need further safeguards mentioned in article 46 of the GDPR, hence it is the most welcome mechanism from a business organisation as it was already mentioned above. In case of no adequacy decision for the UK, the two best suitable transfer mechanisms are standard contractual clauses (SCC) and binding

[18] The EU Court of Justice invalidates EU-US Privacy Shield [online]. In: *dataprivacymanager.net*. 21. 7. 2020. [cit. 9. 1. 2021]. Available at: https://dataprivacymanager.net/the-eu-court-of-justice-invalidates-eu-us-privacy-shield/.

[19] The CJEU judgment of 16th July 2020, C-311/18, Schrems II.

[20] ARMINGAUD, Claude-Étienne; MCFADDEN, Noirin; PHIPPEN Keisha. What future for UK-EU data flows? [online]. In: *K&L Gates*. 28. 10. 2020. [cit. 9. 1. 2021]. Available at: https://www.klgates.com/What-Future-For-UK-EU-Data-Flows-10-28-2020.

corporate rules. The SCC can be described as an individual agreement that includes a contractual obligation on the side of the data exporter and importer and it also includes the rights of the individual whose personal data is being transferred. This safeguards GDPR data protection standards, and it is easy and fast to implement SCC in organisations.[21] According to the judgment in the Schrems II case, the SCC are a suitable mechanism for the transfer of personal data to third countries only if they guarantee a level of protection that is essentially equivalent to that guaranteed within the EU by the GDPR and if they are able to sufficiently protect from intelligence and security services to access such data. Another option for a data transfer mechanism is the binding corporate rules (BCR). The BCR can be described as internal rules that govern an international data flow within a multinational organisation. The implementation of BCR is very costly in time and money. Furthermore, it covers the data transfer just in a single organization.[22]

The future will show us how exactly Brexit will affect personal data flows between the UK and EEA. From the above mentioned we can assume that in 2021 an adequacy decision for the UK will be adopted by the decision of the EC, but there are some challenges that I also mentioned above. In an adequacy decision scenario, the change in personal data flows between the UK and the EEA would be almost none. In a non-adequacy decision scenario, the change to personal data flows between the UK and EEA would be pretty significant. There are two mechanisms - SCC and BCR that could be used in order to safeguard GDPR data protection standards. Both of them have some pros and cons, but in the case of the USA after the invalidation of EU-US Data Protection Shield the organisations started to use the SCC[23] and I think it would be the same in the case of the UK in non-adequacy decision scenario.

---

[21] Ibid.

[22] Ibid.

[23] *The EU Court of Justice invalidates EU-US Privacy Shield* [online]. In: *Dataprivacymanager.net.* 21. 7. 2020. [cit. 9. 1. 2021]. Available at: https://dataprivacymanager.net/the-eu-court-of-justice-invalidates-eu-us-privacy-shield/

.

## 4. BIBLIOGRAPHY

[1] HELLMAN, Jessie. Obama: We can't 'build a wall' around globalization [online]. In: *The Hill.* 22. 7. 2016. [cit. 8. 1. 2021]. Available at: https://thehill.com/blogs/ballot-box/presidential-races/288887-obama-slams-trump-trade-ideas-we-cant-build-a-wall-around.

[2] Cross-border data flows [online]. *bsa.org.* [cit. 8. 1. 2021]. https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf

[3] When did Britain decide to join the European Union? [online]. *ukandeu.ac.uk.* 21. 8. 2020. [cit. 8. 1. 2021]. Available at: https://ukandeu.ac.uk/the-facts/when-did-britain-decide-to-join-the-european-union/

[4] The History of the General Data Protection Regulation [online]. *edps.europa.eu.* [cit. 8. 1. 2021]. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[5] WALKER, Nigel. Brexit timeline: events leading to the UK's exit from the European Union [online]. In: *House of Commons Library*. 6. 1. 2021. [cit. 8. 1. 2021]. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-7960/.

[6] International transfers of personal data [online]. *European Commission.* [cit. 8. 1. 2021]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en

[7] Regulation of the European Parliament and of the Council (EU) 2016/679 of 18 April 2018 on on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)

[8] SLINN, Benjamin; DE FONSEKA, Joanna. *Data Protection and Brexit* [online]. In: *Baker McKenzie* [cit. 8. 1. 2021]. Available at: https://www.bakermckenzie.com/-/media/files/insight/publications/2019/12/data-protection-and-brexit.pdf.

[9] MITCHELL, Ewen; SCHENKER, Sarah. C., Brexit: The Future of Data Flow to and from the EEA and the UK [online]. In: GT London Law Blog. 23. 12. 2020. [cit. 8. 1. 2021]. Available at: https://www.gtlaw-londonlawblog.com/2020/12/brexit-the-future-of-data-flow-to-and-from-the-eea-and-the-uk/.

[10] MORRIS, Chris. Brexit deal: What is in it? [online]. In: *BBC News.* 28. 12. 2020. [cit. 8. 1. 2021]. Available at: https://www.bbc.com/news/55252388.

[11] BUNDY-CLARKE, Fiona. *EU-UK Trade and Cooperation Agreement: Implications for data protection law* [online]. In: *Data Protection Report*. 4. 1. 2021. [cit. 9. 1. 2021]. Available at: https://www.dataprotectionreport.com/2021/01/eu-uk-trade-and-cooperation-agreement-implications-for-data-protection-law/.

[12] *Adequacy decisions* [online]. In: *European Commission.* [cit. 9. 1. 2021]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[13] The CJEU judgment of 16th July 2020, C-311/18, Schrems II, ECLI:EU:C:2020:559

[14] *The EU Court of Justice invalidates EU-US Privacy Shield*. In: *dataprivacymanager.net.* [online] 21. 7. 2020. [cit. 9. 1. 2021]. Available ar: https://dataprivacymanager.net/the-eu-court-of-justice-invalidates-eu-us-privacy-shield/

[15] ARMINGAUD, Claude-Étienne; MCFADDEN, Noirin; PHIPPEN Keisha. *What future for UK-EU data flows?* [online]. In: *K&L Gates*. 28. 10. 2020. [cit. 9. 1. 2021]. Available at: https://www.klgates.com/What-Future-For-UK-EU-Data-Flows-10-28-2020.

---



---

# SMART HOME'S DATA, NEW GOLD VEIN?[1]

*MARTIN ZMYDLENÝ*[2]

## 1. INTRODUCTION

I am quite a huge fan of all kinds of modern solutions such as smart devices, the Internet of Things and smart homes. Even though I do not understand all (most) of the technical aspects of these things, I still consider myself as someone who knows and follows the newest trends. Well, except TikTok, that is something I just do not understand…

Nowadays, things which we never imagined are connected through the internet among themselves. Acquiring and collecting our data, which are then used by manufacturers of these devices to "improve" their customer services. Some companies collect and use more data than others. In the end, the customer, the house owner, mostly does not even know which data is collected, because we all know, how people "read" terms and conditions on the Internet. So lets find out why we love smart solutions and why we want our houses to become smart even though the disadvantage of losing privacy is enormous.

## 2. WHAT IS THE INTERNET OF THINGS (IOT) AND WHY IT IS IMPORTANT TO SMART HOMES?

In a nutshell, a smart home is an interconnected network of various devices based on the Internet of Things (IoT). When a lot of people hear about the Internet of Things, they think the IoT only includes "things." So, if we use the terminology of our Civil Code in section 489: *"A thing in legal terminol-*

---

[1] Esej byla zpracována v semestru podzim 2020 v rámci předmětu MVV1368K Privacy and Personal Data na téma Smart everything. / The essay was written in the autumn 2020 semester for the course MVV1368K Privacy and Personal Data on the topic of Smart everything.

[2] Martin Zmydlený je studentem Právnické fakulty Masarykovy univerzity. Kontakt: 405111@mail.muni.cz.

*ogy is everything that differs from a human being and serves humans."*[3] Quoting more legal definitions of things will not be necessary, it is mostly the same. Well except the definition from Roman law where, as a thing, were considered human slaves. The point is, in our legal knowledge we know "things" as things, stuff, belongings – inanimate objects. But in the terminology of the Internet of Things, the part of the network can be even humans or animals! *"A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network."*[4] This means people and animals can be a part of IoT, even though they aren't exactly things.

The whole ecosystem of IoT is growing and will be enormous including billions and billions of devices connected through various sensors or communication hardware. These devices will be collecting data about their users to improve enjoyment and benefits from using smart devices on the Internet of Things. IoT devices will share their collected data with other devices connected to the web and on behalf of acquired information, other devices will behave and act without the need of human assistance.

For example, when we run out of milk, the fridge will add milk to our shopping list on our smartphones. In another scenario the information about the need for milk can be sent to a delivery service like Rohlík.cz in the Czech Republic or to Amazon in the US and Jeff Bezos will send some of his drones[5] with the needed milk.

IoT should help us live and work smarter, and also help us have more time for our family, our hobbies by solving some of the easy tasks for us, maybe even without us noticing anything.

---

[3] Section 489 of the Act No. 89/2012 Sb., Civil code.

[4] GILLIS, Alexander S., Definition– internet of things (IoT), In: *IoT Agenda* [online]. [cit. 18. 6. 2021]. Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[5] Amazon Prime Air [online]. [cit. 18. 6. 2021] Available at: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

## 2.1 FROM SMARTPHONE TO SMART HOME. FROM SMART HOME TO DUMB FOE?

Although it sounds pretty melodic, the smarter devices are, the dumber are people. If not dumber, we rely more on our smart devices than on our knowledge and skills. I can see it on myself, even if I drive a known route to my mother's home, I rather use GPS navigation on highways, because one can never know what can be ahead. My father never used GPS navigation back some 10 or 20 years ago, and we always found our final destination in Italy, Croatia and elsewhere. But now he also tends to use the navigation on his smartphone, because it is so much easier to follow a route on a smartphone's screen, which would recalculate a better route if something happened than to be stuck in a traffic jam on a highway for hours and then start looking in the map for a possible detour. Is it because we know less than before? No, it is not, we only got used to it and these devices make our lives easier so we use them.

I like the image of a man from probably the 80s or 90s standing with like 20 devices and the description: "*Everything in this picture is now in your pocket."* [6] We very quickly got used to our smartphones solving many of our troubles. We do not need a PC to surf the internet, we do not need a camera for photographs or videos, we even do not need tape measures for measuring or a spirit level. That and all others are in our smartphone and they work very well. (My shelves are in top horizontal shape, thank you iPhone). Due to the habit of using smartphones, smart homes do not seem like something new to us. It is just that we, as people, make another huge part of our life smarter and easier to use.

Technological giants like Apple with Apple HomeKit, Google Home from Google, Amazon's Alexa are now the most trending smart home ecosystems. Companies don't invent smart home ecosystems only to make the life of their customers easier. There is another reason. The numbers of smart homes differ, but there is one thing everyone agrees with and that is the value of smart home devices growing a lot and we are just only at the

[6] The described meme [online]. [cit. 18. 6. 2021]. Available at: https://imgur.com/gallery/NQvsYvd

beginning. The most expected scenario is around 12 - 16% of growth every year from USD 80,83 billion in 2019 to USD 207,88 by 2027.[7] Or USD 66,4 billion in 2019 to USD 175,98 billion by 2025.[8] In the year 2025, there should be around 300 million smart homes in the world. [9] It isn't only that people are lazier or less clever, but it is also caused by lower expenses[10] with acquiring smart home ecosystems and devices. A positive (or negative?) thing about various smart home ecosystems from different companies is the incompatibility among them. This means the companies would need to work together to find solutions for their devices to work on other platforms or we will end up with iDevices working only with Apple's HomeKit and Android devices running only on Google.

The benefits of using smart homes are tremendous and the mostly known. For example, all home devices can be managed by one device in one place. With smart cameras linked to the homeowners' phones, you can always keep an eye on your home. Energy efficiency with a smart thermostat, which will learn our schedule and lower the temperature when we aren't home and adds heat when we watch TV. Lights can turn off when we forget to turn them off and leave the house. The fridge, which can call Bezos's drones, can set the right temperature based on its fullness and type of goods stored in.

The other side of the coin is that all devices collect data and then share them among themselves which means big uncontrollable customers data flows. But where can that data go?

---

[7] Smart Home Market Worth $ 207.88 Billion, Globally, by 2027 at 13.52% CAGR: Verified Market Research. *In: prnewswire.com* [online]. [cit. 18. 6. 2021]. Available at: https://www.prnewswire.com/news-releases/smart-home-market-worth--207-88-billion-globally-by-2027-at-13-52-cagr-verified-market-research-301165666.html

[8] Statista: Smart Home worldwide – statistic [online]. [cit. 18. 6. 2021]. Available at: https://www.statista.com/outlook/283/100/smart-home/worldwide#market-revenue

[9] Ibid.

[10] Ibid.

## 3. SMART HOME'S DATA, NEW GOLD VEIN?

As I mentioned in the last part, data collected from smart devices in a smart home ecosystem will be tremendous. Because I am not an IT expert, I borrowed for describing various data collected by IoT devices from an IoT development company called Digiteum.[11]

First are status data. These data are about basic information like if a device is turned off or on. This is useful for overall planning for maintenance, decision-making and others. Status data must be paired with other IoT data otherwise they are worthless.

Location data are data known to everybody from our smartphones. Location data contains locations of devices and their movement.

Automation data. Type of data that helps IoT systems to control smart home devices, vehicles on the road and other moving objects in the IoT ecosystem. These data are crucial because if data from one device does not work perfectly, the whole ecosystem is at stake.

Actionable data are extensions of status data, but they do not only collect status data, but processes them and transform them into instructions. These data are often used for lowering energy consumption, efficiency optimization and are used for long-term decision-making.

The meaning of this little technical insert is that data from the IoT ecosystem of our smart home are diverse and can be very specific. Status data that track if a device is turned off or on, can look a little worthless. But if we consider these data can be collected e.g. from alarm device, then it is pretty valuable information.

Similarly with my favourite smart fridge. Information on how much milk we drink, the food we eat, is not valuable for most subjects. But if this information is used in a targeted advertisement by our ecosystem provider or a third party, it can be pretty valuable. Another thing is that governments can be curious about these data as well. In the US, which is the lea-

[11] How Does IoT Data Collection Work?. In: digiteum.com. [online] 13.2.2020 [cit. 18. 6. 2021]. Available at: https://www.digiteum.com/iot-data-collection/

ding market of smart homes,[12] there are already known cases, when the police obtained information from Amazon Echo to solve a murder, same as from FitBit.[13] Amazon's acquisition Ring is known for its cooperation with police, the doorbell company changed from "DoorBot" to a device surveilling the suburbs and partnering with the police.[14]

Yes, these scenarios help to solve crimes and the data from smart homes are used by a "third party" for common good, but it does not have to be that way…

## 4. CONCLUSION

In this essay, I tried to describe how we as a people rely on our smart devices and why we tend to also rely on our smart homes. What the possible benefits of smart homes are, but also what the main disadvantage of smart home is or rather the danger of smart homes. Collected data can help us to customize our smart homes, but the costs of possible data breach and data abuse are a real threat.

Collected data can be abused by a collector, the company with the smart home ecosystem. Or rather can be stolen by hackers. The government would also want to get our data for their own use.

Another problem I see with IoT and smart homes is the possibility of corrupting one device, which can lead to corruption of the whole ecosystem like if we get corrupted by some virus on our phone, we can infect the whole smart home and stolen data can be very crucial.

In conclusion, I would say smart homes will have a great positive impact on our daily lives, but we need to try to secure our collected data because problems associated with data breaches can be terrible.

---

[12] Statista: Smart Home worldwide – statistic [online]. [cit. 18. 6. 2021]. Available at: https://www.statista.com/outlook/283/100/smart-home/worldwide#market-revenue

[13] WHITTAKER, Zack. Many smart home device makers still won't say if they give your data to the government. In: *Tech Crunch* [online]. 11.12.2019 [cit. 18. 6. 2021] Available at: https://techcrunch.com/2019/12/11/smart-home-tech-user-data-government/

[14] HASKINS, Caroline. How Ring Went From "Shark Tank" Reject to a America's Scariest Surveillance Company. In: *vice.com* [online]. [cit. 18. 6. 2021] Available at: https://www.vice.com/en/article/zmjp53/how-ring-went-from-shark-tank-reject-to-americas-scariest-surveillance-company

## 5. BIBLIOGRAPHY

[1] Act No. 89/2012 Sb., Civil code.

[2] GILLIS, Alexander S., Definition– internet of things (IoT). In: *IoT Agenda* [online]. [cit. 18. 6. 2021]. Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[3] Amazon Prime Air [online]. [cit. 18. 6. 2021] Available at: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

[4] Smart Home Market Worth $ 207.88 Billion, Globally, by 2027 at 13.52% CAGR: Verified Market Research, *In: prnewswire.com* [online]. [cit. 18. 6. 2021]. Available at: https://www.prnewswire.com/news-releases/smart-home-market-worth--207-88-billion-globally-by-2027-at-13-52-cagr-verified-market-research-301165666.html

[5] Statista: Smart Home worldwide – statistic [online]. [cit. 18. 6. 2021]. Available at: https://www.statista.com/outlook/283/100/smart-home/worldwide#market-revenue

[6] How Does IoT Data Collection Work? In: digiteum.com. [online]13.2.2020 [cit. 18. 6. 2021]. Available at: https://www.digiteum.com/iot-data-collection/

[7] WHITTAKER, Zack. Many smart home device makers still won't say if they give your data to the government. In: *Tech Crunch* [online].11.12.2019 [cit. 18. 6. 2021] Available at: https://techcrunch.com/2019/12/11/smart-home-tech-user-data-government/

[8] HASKINS, Caroline. *H*ow Ring Went From "Shark Tank" Reject to a America's Scariest Surveillance Company. In: *vice.com* [online]. [cit. 18. 6. 2021] Available at: https://www.vice.com/en/article/zmjp53/how-ring-went-from-shark-tank-reject-to-americas-scariest-surveillance-company

---



---