

PREVENTING TERRORISM OR ELIMINATING PRIVACY? RETHINKING MASS SURVEILLANCE AFTER SNOWDEN REVELATIONS

Abstract

After Edward Snowden's leaks revealed to the public in June 2013, mass surveillance programs still exist. Considering that these practises restrain the right to privacy, there is a need to rethink the very concept of mass surveillance. The aim of this paper is to analyse this concept, sum up the problems related to its logic and methods, and question its legitimacy. Critical approach to the concept of mass surveillance is necessary on order to create the basis for resolving current issues related to it.

My research shows that there are reasons to question legitimacy of mass surveillance as it not only breaches the right to privacy but also ignores the presumption of innocence and there is possibly a substantial lack of oversight by the independent bodies which is necessary to make these practices democratic. Moreover, given that mass surveillance programs were introduced to fight terrorism and crime, it should be assessed how efficient they really are and whether they are worth having considering their drawbacks and potential dangers for the society.

Key words: *mass surveillance, terrorism, Snowden, privacy.*

1. Introduction

Information revealed by the former US National Security Agency employee Edward Snowden and published by The Guardian, The New York Times and other media in June 2013 confirmed the existence of surveillance programs conducted by intelligence services such as the US National Security Agency (NSA) and British Government Communications Headquarters (GCHQ). Even though the news about the existence of systems which are monitoring private communications isn't completely new, and the general public was aware of a global system for the interception of

¹ Assistant Researcher, Institute of criminological and sociological research, Belgrade; mail: ivana.stepanovic@gmail.com

private and commercial communication ECHELON since 2001, what made Snowden's revelations shocking was the scale of this surveillance, but also the undemocratic way it was introduced and conducted under secret authorisation². It was revealed that the intelligence agencies had been holding whole populations under surveillance and that targets were not just those suspicious of committing crimes and terrorism acts, but also ordinary citizens as well as political leaders, UN officials and companies.

One of the key questions that arose immediately after Snowden's revelations was the one related to the right to privacy. Due to the development of technology, ubiquitous computing and contemporary surveillance methods, privacy has become a critical topic in the field of politics and law, but one of the main problems seems to be lack of definition of the notion itself and the absence of a clear approach in dealing with privacy related issues. Many theoreticians claim that it is a social construct and therefore its meaning depends on the specific historical and cultural context, however, it also seems that there is some kind of consent that it is something valuable all human beings feel the need for and are entitled to³. After Snowden's leaks, it became apparent that we should rethink the concept of privacy and find some kind of a method of balancing it with conflicting interests. Most importantly, we need to establish some kind of attitude towards the right to privacy versus mass surveillance in order to provide adequate solutions in the sphere of law.

Another key issue that needs to be addressed in relation to mass surveillance is its benefits for fighting terrorism and crime. As Snowden's leaks suggest, it is highly likely that benefits of mass surveillance are simply not worth it. Calculating costs and benefits of surveillance is crucial for determining the attitude that should be taken towards both privacy and surveillance.

Even though it was bureaucratic surveillance developed in previous centuries that led to its modern day practises, with digital technology surveillance reaches mass scale level and possibly covers almost the entire electronic communication of everyone in the world. Since technology inevitably changes the way we communicate and live, it also changes surveillance practises and thereby our very perception and expectation of privacy. If we accept that it is a social construct, we should also accept that we need to build its new meaning, considering the new circumstances. There seem to be two opposing arguments which summarise today's views on privacy and surveillance. The first one says that there is "nothing to hide" and it prioritises security, while the other one claims that privacy is "lost"

² D. Wright, R. Kreissl. *European Responses to the Snowden Revelations: A Discussion Paper*. IRISS, European Commission 2013., 6.

³ C. Bennett. *The Privacy Advocates*. MIT Press, Cambridge Massachusetts 2008., 2

and that we should somehow reclaim it⁴. These is also a medium approach which focuses on finding a balance between the two opposites, admitting that control is a necessity, but only if conducted in a democratic way with respect for privacy rights.

However, after Edward Snowden's revelations it is also important to rethink surveillance as a means of control and question legitimacy of mass surveillance in particular. Considering constant breaches of the right to privacy and restraining liberties, it is crucial to critically approach this issue. This aim of this paper is to sum up potential problems related to mass surveillance and question its legitimacy, especially regarding its efficiency in preventing criminal activities as well as adequate surveillance oversight.

2. The Origins of Mass Surveillance

As Dandeker writes, surveillance practices existed in all societies simply because they are "features of all social relationships", and he stresses out that the key change that brought about the contemporary model of surveillance occurred when personal and patronage forms of indirect control were replaced by bureaucratic systems of administrative power.⁵ He defines surveillance as collection and storage of information about people or objects and the supervision of the activities of people or objects, but also stresses out that it is often used as an administrative means of reproducing a social system of rule.⁶

And it is indeed hard to imagine modern nation states functioning without mass surveillance which have to regulate their internal and external peace with military and police. The ultimate purpose of governmental surveillance has always been maintaining peace or preventing and sanctioning rule breakers. Moreover, the same principle was applied to other institutions including schools, hospices and modern business companies. Due to large numbers of individuals, the only way to make sure everyone obeys the rules was to introduce surveillance systems. Surveillance was the survival strategy of the modern nation state as it would easily collapse without various systems of bureaucratic control⁷. In that sense it can be said that there is nothing wrong with mass surveillance as it is simply an instrument of organising the society. As long as the surveillance is localised, justified and just, it is not a practice that necessarily has to be seen as a threat.

⁴ D. Solove. *Nothing to Hide: The False Tradeoff between Privacy and Security*. Yale University Press, New Haven and London 2011

⁵ C. Dandeker. *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*. Cambridge: Polity Press 1994., 193-194

⁶ *Ibid.* 37-38.

⁷ *Ibid.* 194

Foucault defined modern societies as ‘disciplinary societies’⁸. Its surveillance mechanism was inspired by Bentham’s ‘panopticon’ prison based on the principle of the invisible watcher who watches the prisoners without being seen in order to control or discipline their behaviour by creating an optical illusion that they are being watched at all times. He connects the notion of surveillance to that of power and acknowledges that the key feature of modernity is breaking up the singular governmental centre of power into separate units or centres of power. In this sense all these centres such as schools, factories, medical institutions and prisons are exercising disciplinary power thereby controlling the private lives of the citizens.

While societies of the age of modernity operated with visual and mechanical technology to conduct surveillance practices and the control was limited to specific physical places where surveillance was practised, today’s digital technology makes the surveillance ubiquitous. Deleuze described postmodern societies as “societies of control” as opposed to Foucault’s disciplinary societies.⁹ He stresses out that technology does not determine social forms but rather expresses them: “the old societies of sovereignty made use of simple machines – levers, pulleys, clocks; but the recent disciplinary societies equipped themselves with machines involving energy with the passive danger of entropy and the active danger of sabotage; the societies of control operate with machines of a third type, computers, whose passive danger is jamming”¹⁰.

By calling the new type of societies which emerge with ubiquitous computing, Deleuze anticipated consequences of both new forms of production and new surveillance practices followed by it. In this short article which was published in 1990 he gave a brief prediction of the future of the capitalism and it seems apparent that the societies of control as he defines them should be directly developed from the disciplinary societies and their modes of production and surveillance. He claims that Kafka’s *Trial* is positioned at “the pivotal point between two types of social formations, and described the most fearsome of juridical forms”¹¹ which clearly shows that he sees modern methods of control stemming from bureaucratic surveillance.

While many see technology as the main cause of the spread of surveillance and elimination of privacy in contemporary societies, Deleuze along with many other theoreticians points out that it is not technology that brought about surveillance, but rather social systems developed and used technologies in such a way to design certain systems

⁸ M. Foucault, *Discipline and Punish: The Birth of Prison*. New York: Vintage Books 1995., 205

⁹ G. Deleuze. “Postscript on the Societies of Control”, *October*, Vol. 59, 1992., 3-7

¹⁰ *Ibid.* 6

¹¹ *Ibid.* 5

of control. It is very common nowadays to associate surveillance with technology, but it is simply not seeing the bigger picture, as the story about surveillance begins long before computers were invented.¹² It was in fact control that motivated creation of computers which are enabling information collection and processing and the development of these technologies started back in the 19th century with the invention of tabulating machines by Herman Hollerith and others.¹³ After World War I, these machines were used not only by governmental institutions, but also for businesses (for example, IBM punch card machines were used to organise and control enterprises)¹⁴.

It was during 1960's and 1970's when the discourse of contemporary surveillance started to emerge along with creation of databases of both governmental institutions and business companies which wanted to collect data on consumers.¹⁵ This means that the surveillance system we now live in and which we became more aware after Edward Snowden's revelations in 2013, was actually conceived and structured long before, and it is new technologies that took it to the new level in terms of quantity of collected information.

3. What is wrong with Mass Surveillance?

It can be argued that the underlying principle of surveillance remained the same even though technology radically changed the way it operates. It seems that the key difference between monitoring practices in earlier centuries and today is the scale of surveillance. The capacities of collecting information on people has dramatically increased and in Edward Snowden's words the problem with NSA databases is the "omniscient, automatic, mass surveillance" of everyone, regardless of whether they are suspected of any wrongdoing.¹⁶ Bulk collection of private correspondence, interception of telephone calls and storage of various personal data in huge databases not only violates the right to privacy as a fundamental right, but also doesn't recognise the presumption of innocence by treating ordinary people as potential suspects.

Human rights are considered as pillars of democracy which is why they should not be violated unless there is a good reason. The purpose of mass surveillance projects imposed by the NSA is fighting terrorism and

¹² D. Barnard-Wills. *Surveillance and Identity: Discourse, Subjectivity and the State*. Farnham: Ashgate 2012., 12

¹³ D. Wright et al. *Surveillance, Fighting Crime and Violence*, IRISS, European Commission 2013., 28

¹⁴ *Ibid.* 29

¹⁵ *Ibid.* 30

¹⁶ Ted Talks, *Edward Snowden: Here is How We Take Back the Internet*, http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet, 03.05.2015.

security was put forward as the core value in every society which should be considered as more important than privacy. However, the question which arises in the light of Snowden's revelations is this: is it really necessary to trade all privacy for security?

The so called "trade-off paradigm" has been extensively debated in the domain of legal theory, and in 2010 the European Commission questions the trade-off model between privacy and security through the PRISMS Project. The objectives of the project were to determine whether people actually evaluate the introduction of security technologies in terms of a trade-off and what are the main factors that affect public assessment of the security and privacy implications of given security technology. The survey was conducted in 27 EU countries with target population being general population aged 18+ and included 27,195 interviews. The results of this survey had shown that European citizens consider privacy as an important value (both online and offline), that people feel more data about them is collected and that they less accept disclosure of personal data compared to previous surveys. The general conclusion was that "there is no significant relationship between citizens' general attitudes towards 'privacy' and 'security'"¹⁷.

The PRISMS Project clearly shows that the trade-off paradigm is not the only way to understand the problem of surveillance. The debate on privacy does not end with a simple question of whether people are ready to exchange their individual privacy for the benefit of security of the society as a whole. The results of this survey point towards a view that the two issues should be tackled separately since the general public in the EU values both privacy and security. In this sense, mass surveillance that wipes out individual privacy is deeply disturbing.

However, one of the crucial problems related to the NSA surveillance programs is the fact that their legality is based on "decisions made by secret judges in secret courts and secret interpretations of law"¹⁸ He refers to the Foreign Intelligence Surveillance Court (FISC) which "operates in complete secrecy"¹⁹. The Guardian journalist Glenn Greenwald's questioning of the transparency of this court was based on the analysis of NSA documents provided by Edward Snowden. He claimed that "those documents demonstrate that this entire process is a fig leaf, 'oversight' in name only" and that this court "offers no safeguards"²⁰

¹⁷ M. Friedwald, "Key results from the PRISMS survey", *PRISMS Project*, http://prismsproject.eu/wp-content/uploads/2014/11/Friedewald_PRISMS@FinalConference.pdf, 03.05.2015.

¹⁸ TED Talks, *Edward Snowden: Here is How We Take Back the Internet*, http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet, 03.05.2015.

¹⁹ G. Greenwald, "Fisa court oversight": a look inside a secret and empty process", *The Guardian*, <http://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy>, 03.05.2015.

²⁰ *Ibid.*

The documents show that the NSA does not in fact need to inform the court on whose calls and emails they intend to intercept in order to obtain approval from the FISC. In this way Surveillance programs can listen to great many different calls and read great many emails without any requirement of a warrant, as limitations are applied only to surveillance of US citizens and communications that occur within USA borders²¹. “The decisions about who has their emails and telephone calls intercepted by the NSA is made by the NSA itself, not by the Fisa court, except where the NSA itself concludes the person is a US citizen and/or the communication is exclusively domestic. But even in such cases, the NSA often ends up intercepting those communications of Americans without individualized warrants, and all of this is left to the discretion of the NSA analysts with no real judicial oversight”.

In their discussion paper published as a part of European Commission’s IRISS program, Wright and Kreissl call the FISC a “toothless” court which “provides a prima facie legal basis for many NSA actions, but they hollow out the idea of rule of law by doing so”²² The Increasing Resilience In Surveillance Societies (IRISS) project was initiated by the European Commission after the Snowden revelations with the aim to investigate and analyse surveillance and its impact on human rights, as well as to provide ideas for enhancing social, economic and institutional resilience in Europe.

If there is no independent judicial instance that ensures transparency and accountability of the surveillance practices, governments and intelligence services have virtually limitless power to monitor citizens. This type of unrestrained control cannot be called democratic and was always associated with autocratic regimes throughout history. The fact that mass surveillance programs were introduced secretly, without public awareness and consent illustrates just how severely this type of control undermines basic principles of democracy.

Worryingly, this type of control essentially targets everyone and not just those suspected of committing crimes, planning terrorist attacks or being involved with extremists. Data provided by Edward Snowden confirm fears that many innocent citizens were targeted for all sorts of reasons other than preventing terrorist attacks and crime.²³ One of the worst consequences of mass surveillance programs is their abuse. As Stephen Walt, Harvard professor of international affairs stated: “Once a secret surveillance system exists, it is only a matter of time before

²¹ *Ibid.*

²² D. Wright and R. Kreissl. *European Responses to Snowden Revelations: a Discussion Paper*. IRISS, European Commission 2013.,14

²³ *Ibid.*

someone abuses it for selfish ends”²⁴. This is why oversight of these programs is essential in every democratic state.

After Edward Snowden revealed NSA documents that prove the existence of mass surveillance projects such as NSA’s PRISM and GCQH’s TEMPORA, it was also discovered that leaders of Germany, Italy, Spain and other allies were targets of surveillance programs, it became apparent that it was not used solely for the purpose of fighting terrorists. It was also learnt that much of the NSA surveillance was focused on oil companies which also clearly signalises abuse of these practises.²⁵

While rarely anybody would argue that all forms of surveillance are harmful, key criticisms of mass surveillance practises revolve around the argument of “failure of oversight”. Wright and Kreissl underlined this problem and pointed out that surveillance should be controlled and targeted to battle terrorism.²⁶ Consequently, it is not surveillance *per se* that poses a threat to democracy, but the lack of control of surveillance practises as well as bulk collection of data on individuals who are not suspects. Wright and Kreissl propose that “there should be no mass surveillance unless any particular system can be justified, starting with a privacy impact assessment, review by a regulatory authority and parliamentary oversight committee” and add that this oversight committee should be led by a member of opposition.²⁷ Additionally, they say that governments should conduct regular opinion surveys to find out what the public thinks about the extent of surveillance and to produce independent annual reports on the state of privacy and surveillance along with recommendations on how to provide better protection of privacy.²⁸

Furthermore, the problems with surveillance and control over individual privacy does not end with monitoring electronic communication. The very last bastion of privacy should be inside of the mind to which only individuals should have exclusive access. However, Defence Advanced Research Projects Agency (DARPA) works on projects of mind control for military purposes.²⁹ Even though these projects are still on experimental level, there is a strong indication that the neuroscience can contribute to inventing mechanisms for invading the innermost area of privacy – the inside of the

²⁴ S. Walt, “Snowden deserves an immediate presidential pardon”, *Financial Times*, <http://www.ft.com/cms/s/0/0ccf2d14-e7c1-11e2-babb-00144feabdc0.html#axzz3YzuAMGSb>, 03.05.2015.

²⁵ G. Greenwald. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London: Penguin 2013., 151

²⁶ D. Wright and R. Kreissl. *European Responses to Snowden Revelations: a Discussion Paper*. IRISS, European Commission 2013., 43

²⁷ *Ibid.* 43

²⁸ *Ibid.* 43

²⁹ E. D. Cohen. *Mass Surveillance and State Control: The Total Information Awareness Project*. Palgrave Macmillan 2010., 16-17

human brain. With possibilities of these practises arises the fear of realisation of the most disturbing Orwellian prediction – the “thought police”. The world sleepwalked into mass surveillance of electronic data and unless there is a substantial change in the way surveillance practices are conducted, privacy might be eliminated altogether, followed by all freedoms.

4. Questionable Success of Mass Surveillance in Fighting Terrorism and Crime

The reasoning behind programs for mass surveillance is that these systems will provide new, more efficient form of policing which will enable more crime prevention. Anti-terrorism legislations such as USA Patriot Act and other legal regulations of different countries around the world that concern intelligence and national security legalised many forms of surveillance in order to protect security and battle terrorism, but the key question is how useful these systems are for prevention of terrorist attacks and crime in general.

If governmental surveillance isn't itself being controlled in any way, as it was shown in the previous chapter, then it is clear that it is hard to measure the impact of surveillance on crime prevention. This is one of the key conclusions stated in the IRISS on surveillance, fighting crime and violence.³⁰ Moreover, Edward Snowden stated that, according to his knowledge and experience during his contract with the NSA, mass surveillance “hasn't stopped a single terrorist attack”.³¹ He also said that terrorism was used as a “cover for action” and that in his personal opinion these surveillance programs do not have any value. Since 2001, the everyday presence of digital surveillance has become normalised through the so called “trade-off paradigm” as the whole world was frightened by acts of terrorism. People were promised to get more security in exchange for some of their privacy.

However, the concept of increasing surveillance for the sake of safety isn't exclusively related to terrorism and issues of national security, but also individual safety. Twentieth century introduces concepts of ‘defensible spaces’ and ‘gated communities’ which illustrates modes of surveillance that are not practised by governments or corporations, but in fact by citizens themselves. As Setha M. Low writes, “At the turn of the twentieth century, secured and gated communities in the United States were built to protect family estates and wealthy citizens [...] gates then spread to resorts and country club developments, and finally to middle-

³⁰ D. Wright *et al.* *Surveillance, fighting crime and violence*. IRISS, European Commission 2013., 11

³¹ TED Talks, *Edward Snowden: Here is How We Take Back the Internet*, http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet, 03.05.2015.

class suburban developments”.³² Her anthropological research revealed that it was the urban fear of the “other” that led to this trend of hiding behind gates and introducing surveillance mechanisms in and around the private property to ensure protection against criminals who were normally referred to as members of other races or lower classes.³³

On the other hand, the architect Oscar Newman introduced the concept of ‘defensible space’ in order to create a new criminological sub-discipline called “Crime Prevention Through Environmental Design” (CPTED). He proposes the idea of creating spatial units which rely on “self-help rather than on government intervention, and [...] it depends on resident involvement to reduce crime and remove the presence of criminals”.³⁴

However, the idea of preventing crime by the means of video surveillance has led to the development of CCTV surveillance system which was first established in the UK and then copied around the world. Video surveillance as we know it today consists of both security cameras in public spaces operated by the police and those installed in private properties including shops and residential buildings. Named ‘the most surveilled country in the world’³⁵, the UK has an extremely high level of video surveillance, but as William Webster claims, the “use of CCTV has evolved from being associated with combating crime to systems designed to reduce the fear of crime, deter anti-social and undesirable behaviour, and encourage community safety”.³⁶ It can therefore be said that it is now commonly accepted that the role of video surveillance is not simply prevention of crime but also controlling behaviour. Similarity with Bentham’s prison guard is obvious.

Since it isn’t possible to have constant live surveillance and have everyone monitored at all times, the possibility of recording and storing video files is useful for identifying and tracking criminals after the crime has occurred, as well as providing sufficient evidence for the prosecution.

Other key surveillance areas aimed at fighting crime and terrorism include DNA samples, biometrics, x-ray security screenings etc. Information collected from mobile phone service providers are also used by the police and secret services to fight terrorism and other forms of crime. However, the major problem with all these surveillance practises seems to be a lack of

³² S. M. Low, „The Edge and the Center: Gated Communities and the Discourse of Urban Fear“, S. M. Low and D. L. Zuniga eds. *The Anthropology of Space and Place*. Malden, Oxford, Carlton: Blackwell Publishing 2007., 388

³³ Ibid. 389

³⁴ O. Newman. *Defensible Spaces*. Department of Housing and Urban Development and Research 1996., 9

³⁵ D. Barnard-Willis. *Surveillance and Identity: Discourse, Subjectivity and the State*. Farnham: Ashgate 2012., 18

³⁶ W. Webster, “CCTV Policy in the UK: Reconsidering the Evidence Base”, *Surveillance & Society*, Vol. 6, Issue 1, 2009.

oversight. In other words, there is no one to watch the watchers.

Using surveillance technologies often leads to breaches of the right to privacy and often doesn't acknowledge the presumption of innocence which is an important legal safeguard.³⁷ This is precisely why it is important to establish some kind of independent monitoring system and constantly analyse the impact of surveillance technologies on preventing crime.

With its IRISS project initiated after Snowden's revelations, the European Commission made a bold statement that there is a need for the increase of resilience on existing surveillance practises and their researches show that there is an "insufficient an incomplete knowledge and consideration of the social and economic costs of surveillance".³⁸ The question seems to be: is mass surveillance really worth it, or is it just a means of control that eliminates privacy without achieving other important benefits for the society? Costs and benefits should clearly be re-evaluated.

It should also be established whether a more targeted surveillance that focuses on crime prevention and detection should replace mass surveillance and bulk collection and storage of private information of ordinary citizens. According to the so called "trade-off" paradigm, citizens should exchange their individual freedom for security which is considered to be greater benefit for both individuals and the society as a whole. But while this sounds as a very reasonable argumentation most people would agree with, Snowden's revelations on surveillance practices done by the NSA and GCHQ imply that there is a need to question this reasoning.

Perhaps there is no need for a trade-off and citizens can enjoy both their human right to privacy and have security. This is merely a hypothesis based on some researches and hints dropped by Edward Snowden himself, but it could be proven wrong or right with a research that would weigh the impact of mass surveillance on preventing terrorism and crime, and assess whether it is worth it at all or not.

The very existence of these programs that enable surveillance on such a mass scale without proper oversight is worrying because it opens up endless possibilities for abuse. Unlocking channels of communication and disabling encryption potentially makes these channels and databases vulnerable and leaves personal information of citizens more exposed to criminals. In this sense surveillance systems can perhaps cause more criminal activities instead of actually preventing them which would make societies even less safe, while at the same time depriving individuals from privacy.

³⁷ D. Wright *et al.* *Surveillance, fighting crime and violence*. IRISS, European Commission 2013., 12

³⁸ *Ibid.* 14

5. Conclusion

Surveillance not a modern day phenomenon, but rather a type of practice that was exercised throughout history in very different communities. However, contemporary mass surveillance is a new thing that emerged with rapid development of digital technology. Even though new technologies facilitate electronic surveillance on such a mass scale, it is not technology itself that caused. Surveillance as we know it today stems from bureaucratic systems established in modernity and the principle which existed a century ago remains exactly the same, while it is simply the technology that speeds up the process and allows collecting more data.

But while it seems obvious that there is nothing wrong with surveillance *per se*, there are certain problems with both the logic and the method of conducting mass surveillance. As it applies to both suspects and innocent citizens, it breaches the right to privacy and ignores presumption of innocence. Moreover, as some researches have shown, that there is a reason to question the impact of mass surveillance programs and collecting bulk data on prevention of terrorism and crime which is supposed to be the only reason why such programs were established in the first place.

Another big problem with mass surveillance is the lack of control of these practices by independent instances. These should be courts such as FISC in USA, but, as this paper and many other documents show, there is a strong doubt that these courts are actually not independent and that they are not a much needed safeguard against unlawful surveillance of innocent individuals. This issue leads to questioning the legitimacy of mass surveillance due to the lack of oversight. Unless surveillance practises are monitored and regulated by the independent body, these practices are simply not democratic. Furthermore, the fact that very little has changed in the legal system to stop such surveillance practises almost two years since Edward Snowden's first leak shows how powerful and undemocratic this system already is.

The consequences of such undemocratic practices are also worth considering. Allowing uncontrolled mass scale surveillance may potentially lead to even more severe forms of control than simply recording and storing electronic data. Considering the nature of developments in the field of neuroscience conducted by institutions such as DARPA, mind control isn't a science fiction any more, but quite possibly a realistic fear. Control practices could potentially evolve into losing even more freedom and wiping out all spheres of privacy, including the privacy of mind.

Finally, "nothing to hide" argument which is based on a belief that innocent people have nothing to hide and therefore should not be opposed to losing their privacy should be questioned as well. The very concept of human

rights is constructed on the belief that all humans need them and that they are somehow inherent to the human nature. In the words of Edward Snowden, “you need your rights because you never know when you are going to need them”.³⁹

It is for all these reasons that the concept of mass surveillance should be critically approached rather than just accepted and that steps should be taken to assess its potential dangers as well as benefits.

Ivana Stepanović, master

istraživač pripravnik

Institut za kriminološka i sociološka istraživanja, Beograd

SPREČAVANJE TERORIZMA ILI ELIMINACIJA PRIVATNOSTI? KRITIČKO PREISPITIVANJE MASOVNOG NADZORA NAKON OKTKRIĆA EDVARDA SNOUDENA

Rezime

Nakon otkrića Edvarda Snoudena juna 2013 godine, programi za masovni nadzor i dalje postoje. S obzirom na činjenicu da ove prakse ograničavaju pravo na privatnost, postoji potreba da se sam koncept masovnog nadzora kritički promisli. Cilj ovog rada je da analizira ovaj koncept, sumira probleme vezane za njegovu logiku i metode nadzora, kao i da preispita njegovu legitimnost. Kritički pristup fenomenu masovnog nadzora je neophodan kako bi se stvorila baza za rešavanje aktuelnih problema vezanih za ove prakse.

Ovo istraživanje pokazuje da postoje razlozi da se preispita legitimnost masovnog nadzora, i to ne samo zato što on krši pravo na privatnost, već i zato što ignoriše pretpostavku nevinosti i veoma je verovatno da ne postoji adekvatna kontrola od strane nezavisnih tela nad samim sistemima masovnog nadzora koja bi ga učinila demokratskim. Štaviše, kako je masovni nadzor uveden u cilju borbe protiv terorizma i kriminala, potrebno je proceniti koliko je on u tome efikasan i da li se uopšte isplati, s obzirom na manjkavosti i potencijalne opasnosti po društvo koje on sa sobom nosi.

Ključne reči: masovni nadzor, terorizam, Snouden, privatnost.

³⁹ TED Talks, *Edward Snowden: Here is How We Take Back the Internet*, http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet, 03.05.2015.