DOI 10.5817/MUJLT2015-2-3

THE PUBLIC PERCEPTION OF CYBER-SURVEILLANCE BEFORE AND AFTER EDWARD SNOWDEN'S SURVEILLANCE REVELATIONS

by

ALEŠ ZAVRŠNIK[*], PIA LEVIČNIK[**]

The article contextualizes contemporary cyber-surveillance practices in the light of Edward Snowden's revelations of massive espionage by intelligences services and shows the results of an online survey on the public perceptions of privacy in public telecommunication networks in Slovenia. The results relate to types and frequency of victimization; self-reported study on violating of the privacy of others; concern for the protection of one's own privacy; perception of those carrying out surveillance; the value of privacy; views on abrogated data retention regulation; and awareness of personal data protection remedies.

Despite growing distrust of large internet corporations and – after Edward Snowden's revelations – Intelligence agencies, the findings indicate a low degree of awareness and care for the protection of personal data. In regard to the perception of primary subjects of surveillance, 56 percent of respondents chose internet corporations as the greatest threat to their privacy, followed by telecommunications companies (25 percent), and shops with loyalty programs (23 percent). According to chi-square and Cramer's coefficient calculations, gender correlation is weak, but men feel more threatened by foreign intelligence services and the Slovene Intelligence and Security Agency. By comparing responses before and after the Datagate affair, we noted that prior to this date, only a handful of people felt threatened by foreign or domestic intelligence agencies. An increased feeling of threat after this date is evident in men as well as women.

[*] ales.zavrsnik@pf.uni-lj.si, Researcher Associate at the Institute of Criminology at the Faculty of Law in Ljubljana and Assistant Professor at the University of Ljubljana, Slovenia.

[**] pia.levicnik@gmail.com, currently working as a legal counsellor (electronic communication law), occasionally cooperating with researchers from the Institute of criminology (Faculty of law, Ljubljana).

KEY WORDS
Privacy, Personal Data Protection, Public Opinion Survey, Perception of Privacy, The Internet, Social Networking, Snowden, Intelligence Services, Information Commissioner, Data Protection Authority (DPA), Data Retention, Slovenia

1. INTRODUCTION

The deepening of the digital economy is creating a vast amount of personal data. The existing internet business model is built on surveillance.[1] States thus want to access personal data for law enforcement and intelligence purposes, while internet and telecommunications companies want to maximize their profits by monetizing data. Today, the real danger to fundamental liberties, such as privacy, thus lies in new alliances between governments and private companies that are creating the "surveillance-industrial complex".[2]

Edward Snowden's revelations of massive espionage by intelligences services in June 2013 exposed all these dimensions of contemporary surveillance. The revealed information poses several broader questions related to surveillance in the digital age: 1) How should privacy be understood? 2) How should security actors with often overlapping powers be regulated? 3) How should power relations on the internet be understood?

1) The need to understand privacy in a new way has been extensively addressed by prominent scholars in the last decade. For instance, Nissenbaum has claimed that privacy should be understood as "contextual integrity".[3] Her theory of the contextual integrity of privacy is based on the assumption that personal data is always linked to a certain social context, and that in any such context there are specific norms that determine the appropriateness of the disclosure of personal data and the norms of personal data flows. New technologies such as Vehicle Safety Technology (VSC) disrupt the contextual integrity of personal data, either because they violate the norms of appropriateness, or the norms of distribution (Zimmer,

[1] Schneier, B., *Surveillance Is The Business Model Of The Internet*. Viewed December 14 2014. Available at: https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html.

[2] Ball, K., Snider, L. 2013, *The Surveillance-Industrial Complex: A Political Economy Of Surveillance*, Routledge, New York.

[3] Nissenbaum, H. 2004, *Privacy As Contextual Integrity*, Washington Law Review, 79 (2004) 1, pp. 119–158.
Nissenbaum, H. 1998, *Protecting Privacy In An Information Age: The Problem With Privacy In Public*, Law And Philosophy, 17 (1998), pp. 559–596.

2005). For example, VSC technology that allows vehicles to communicate with each other and with road infrastructure enables vehicle tracking, which leads to digital databases on one's whereabouts, paths, and time spent at specific destinations. This clearly exceeds the notion of the reasonable expectation of privacy in public spaces as the technology collects more than only visual and non-specific information about our movements.

A similar attempt to refashion our understanding of privacy has been made by Solove with his theory of a "pluralistic understanding of privacy".[4] Privacy is not a concept with necessary and sufficient elements, he claims, but should be understood as a set of "family resemblances". Orwell's "Big Brother", an overused analogy for contemporary surveillance practices, inadequately captures the contemporary challenges as it focuses merely on data collection. The mysterious ways in which digital data is being collected, stored, traded, and sold puts data subjects in a confusing situation that more resembles Kafka's protagonist Josef K. from the novel The Trial. The predominant problems concerning privacy are related to data processing, as "ordinary" citizens have immense difficulties in identifying the accountable entities benefiting from their personal data. Pursuing "data justice" is as confusing as in court proceedings in The Trial: Who owns personal data? Where is data stored and processed? How can data subjects reach the accountable data controllers and processors while data moves from "cloud" to "cloud" or from one jurisdiction to another, and while it is being traded for different sorts of purposes, without the data subject benefiting from such trade?[5]

2) Snowden's revelations challenge regulatory issues in the "control and security domain".[6] Since the end of the Cold War, boundaries between actors in the "control and security domain" have become increasingly blurred. The military is extensively engaged in missions typical of law enforcement agencies, while the police have become increasingly involved in military missions abroad and domestically, on one hand, and in

---

[4] Solove, D. 2007, *"I've Got Nothing To Hide" And Other Misunderstandings Of Privacy*, San Diego Law Review, 44 (2007), p. 745.

[5] For instance, tweets are being sold to a deep-fat-fryer manufacturer. Viewed 15 January 2015. Available at:http://www.theguardian.com/technology/2014/nov/05/twitter-soggyfries-big-data-advertising.

[6] The blurring of boundaries in the control and security domain has been extensively researched over the last two decades. See an overview in Završnik, A. 2013, *Blurring The Line Between Law Enforcement And Intelligence*, Journal of Contemporary European Research, 9 (1) p. 182-202. Available at: http://www.jcer.net/index.php/jcer/article/view/452.

intelligence operations, on the other.[7] Finally, intelligence agencies as the third entity in the control and security domain are now entrusted with more law enforcement duties, e.g. in the fight against serious crime and terrorism.[8] Such blurring of the boundaries between the main actors in the "control and security domain" puts ordinary citizens in a legally uncertain position.[9] The division between these actors has always been artificial and in flux to some degree, but the contemporary blurring of boundaries disallows the possibility of a firm regulatory framework that would prevent abuses such as those revealed by Snowden.

3) Last but not least, Snowden' revelations indirectly point to a power struggle for control over the internet. According to Schneier, contemporary cyber-surveillance is best understood by distinguishing different centres of power that use new technologies.[10] Governments and corporations are traditional powers, while distributed power occurs in two forms: either as the "negative" power of criminal groups, or the "positive" power of, for instance, dissident groups. Today, the traditional power of governments and corporations is growing exponentially. The development of online social networks, cloud computing services, and the design of devices controlled remotely by manufacturers, along with the general deepening of the digital economy, all strengthen the power of companies. In one way or another, governments gained access to the data collected by these companies. Governments want to strengthen their models of governance with data analytics and algorithms and use new stockpiles of data in various domains, such as policing, where predictive policing aims to determine the location of future crimes based on existing criminal records.

To conclude, these are some of the parameters of the contemporary situation in the cyber-surveillance domain revealed also by Snowden's revelations in 2013. But, how do all three of these broader issues affect the public perception of cyber-surveillance? Public attitudes towards

---

[7] Den Boer, M., Janssens, J., Vanderbeken, T., Easton, M., Moelker, R. 2010, Epilogue, Concluding Notes On The Convergence Between Military And Police Roles, in Blurring Military And Police Roles, eds. Easton, M., Den Boer, M., Janssens, J., Moelker, R., Vanderbeken T., Eleven International Publishing, The Hague.

[8] Lutterbeck, D. 2005, *"Blurring The Dividing Line: The Convergence Of Internal And External Security In Western Europe"*, European Security, 14 (2), pp. 231-253.

[9] See, e.g., Vervaele, J. 2005, *"Terrorism And Information Sharing Between The Intelligence And Law Enforcement Communities In The US And The Netherlands: Emergency Criminal Law?"*, Utrecht Law Review 1 (1), pp. 1-27.

[10] Schneier, B. *The Battle For Power On The Internet*. Viewed 26 January 2015. Available at: http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/.

surveillance technologies vary from technology to technology and between countries. Generally, the public rarely has a chance to appraise all the relevant information about particular technologically enhanced surveillance practices (TESPs), giving rise to highly varied responses to individual surveillance technologies. For often arbitrary reasons, public opinion in different countries may accept some TESPs but passionately oppose others. This paper is an attempt to understand public perceptions of cyber-surveillance in Slovenia. This knowledge has been gained on the basis of the results of an online survey encompassing attitudes towards several surveillance technologies that was conducted in Slovenia in 2012, 2013, and 2014. It shows whether and how Snowden's revelations regarding mass surveillance carried out by the intelligences services of the USA, the UK, and other countries' have changed the general public's attitudes to surveillance.

2. METHODOLOGY

At the Institute of Criminology at the Faculty of Law of the University of Ljubljana, we conducted an online survey (using Google docs) on the use of information technology, cyber crime, and victimization, within the project "Surveillance and Crime Control: Ethical, legal, and criminological aspects of emerging pre-crime detection and surveillance technologies" in the years 2012 – 2014. The online survey consisted of 31 closed questions (interval questions, yes/no questions, tabular questions with multiple choice options, grading tables) and four demographic questions. The analysis is based on responses from the academic year 2012/2013 (October to May) and from the academic year 2013/2014 (October to January). The survey consisted of four sets of questions:

1. Cyber victimization: we asked the participants how they feel about interception of the content of online communications, whether they had experienced abuse of their personal data or if their photographs had been published without their prior consent. We also asked them about self-protective behaviour (e.g. whether they use different types of computer software protection), about their understanding of various online threats, and about their (potential) reactions after being victimized (i.e. we asked them who they would turn to after suffering online victimization).

2. Cyber activities: a self-report study on violations of the privacy of others was conducted. The questions dealt with how or if respondents had violated the privacy rights of others online, especially in social networks.

3. Protection of personal data: we were interested in how concerned participants are with personal data safety in various surveillance domains (e.g. on the internet; in the process of having personal document made; in public spaces monitored by video surveillance systems; regarding use of the "Urbana" city smart card; and in using loyalty programmes offered by retail chains). We asked them about their level of anxiety in relation to various agents of social control, their willingness to submit their personal data for a variety of benefits, their awareness and attitudes towards data retention in public telecommunication networks, and their awareness of different mechanisms that are in place for safeguarding fundamental liberties.

4. Attitudes regarding specific surveillance technologies in road transport (e.g. the respondents' degree of support regarding such technologies) and on the internet (e.g. how they perceive control over their own personal data; privacy settings in social networks, etc.).

The respondents were invited to participate in the survey via e-invitations, either with the help of their faculties (i.e. university school/division) through e-boards or by e-mail. Students were the targeted population; those who took part in the survey were mainly students of the Faculty of Law and the Faculty of Social Sciences of the University of Ljubljana, and the Faculty of Criminal Justice and Security of the University of Maribor.

Data analysis was carried out with the SPSS 15 software.[***] We created two-dimensional frequency (contingency) tables, used Pearson's chi-square test for the calculation of links between variables, the likelihood ratio, Cramer's coefficient, and ordinal logistic regression. A χ^2 test was conducted with a level of significance of a = 0.05 (the limit of probability below which we are able to reject the null hypotheses).

Notwithstanding the fact that when testing the independence of variables on smaller samples the likelihood ratio is generally more accurate, while Pearson's chi-square (χ^2) is typically used in larger samples, we always used both. If χ^2 was smaller than 0.05 with Pearson and larger for the likelihood ratio, we agreed that the variables were not related. For

[***] We would like to thank Bogomil Brvar for providing help with the statistical analysis.

determining the mean values, we created charts of mean values and a 95% confidence interval.

For differences between the sexes we used ordinal logistic regression, where sex, the independent variable, could be male or female, while the dependent variable could take a value anywhere in the interval (1-5).

The first round of surveying was conducted in the academic year 2012/2013, and the sample amounted to 539 (n1). In that particular period we gradually added additional questions and thus we have another sample that answered four questions in the same period (n2 = 481). The second round was conducted in the following academic year, 2013/2014, when we reached a sample of 266 (n3).

3. PRIVACY VICTIMIZATION

Among the various risks on the internet, 66% of respondents perceive the risk of the interception of communications content as quite problematic (on a scale from 1 – not a problem, and 5 – very problematic, 4 or 5 were the most frequent responses), while a whopping 82% of respondents perceive malicious computer software (malware), which is often used to invade privacy, as highly problematic (4 or 5); only child pornography and financial fraud were perceived as more problematic.

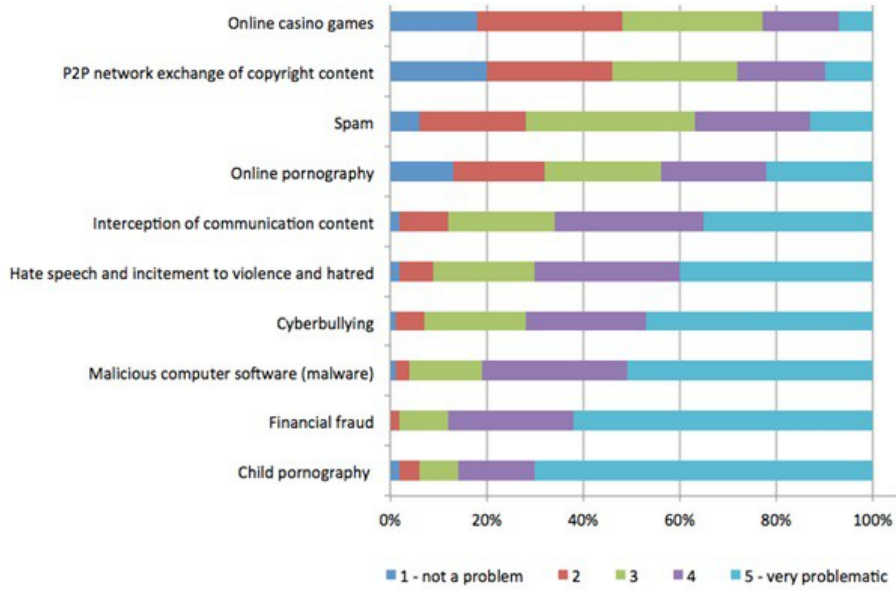


Figure 1: Perceived dangers on the internet

When participants were asked if they had ever experienced internet-related privacy victimization, 9% of respondents revealed that they have been the victim of personal data theft at least once. 23% of respondents had been victimized by unauthorised publication of compromising photographs of themselves (e.g. on Facebook or via e-mail).

We also examined the familiarity of the respondents with computer malware, phishing, botnet networks, credit card skimming, and spyware. 35% of the respondents declared that they knew "quite well" or "very well" the imminent threats to users' privacy posed by spyware (on a scale from 1 – not acquainted and 5 – very well acquainted). This percentage is still not as high as stated familiarity with computer malware, but nevertheless considerably higher than with other online threats.

As self-protective preventive behaviour represents the key solution for all-inclusive privacy protection, we asked the respondents about their computer self-protection measures.

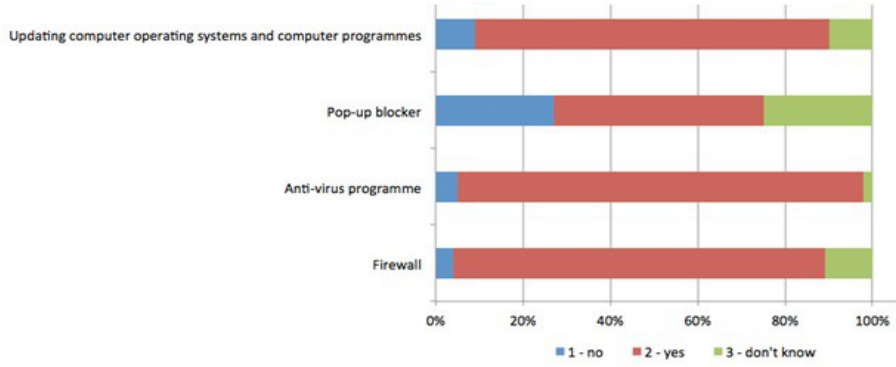


Figure 2: Self-protective measures – prevention

In order to learn about the extent of self-protective behaviour after victimization has already occurred, we asked the respondents whom they would turn to in the event of online threats, such as an unauthorised computer hack, an unexplained crash of a computer system, spam, social network bullying, mobile phone bullying, and personal data abuse.

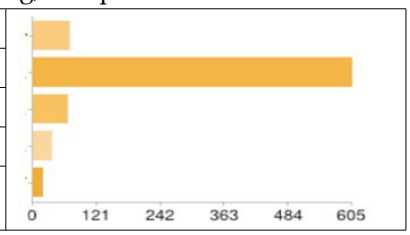
No one	9 %	
Law enforcement agencies	75 %	
Any independent IT expert	8 %	
My internet service provider	4 %	
The Academic and Research Network of Slovenia (Arnes), SICERT	2 %	

Figure 3: Self-protective measures – response in the event of online personal data abuse

In the event of personal data abuse, the respondents revealed a much higher degree of trust towards the police than with other online threats, especially regarding an unauthorised computer hack, regarding which the respondents put their faith in independent experts rather than the police.

No one	16 %
Law enforcement agencies	26 %
Any independent IT expert	38 %
My internet service provider	12 %
The Academic and Research Network of Slovenia (Arnes), SICERT	5 %

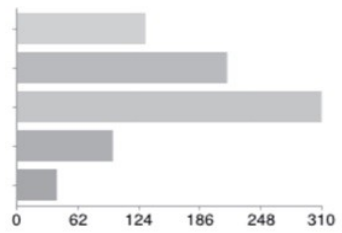


Figure 4: Self-protective measures – response in the event of an unauthorised computer hack

4. SELF-REPORT STUDY ON VIOLATING OF THE PRIVACY OF OTHERS

We asked the respondents whether they had ever violated the privacy of others or exercised other forms of surveillance.

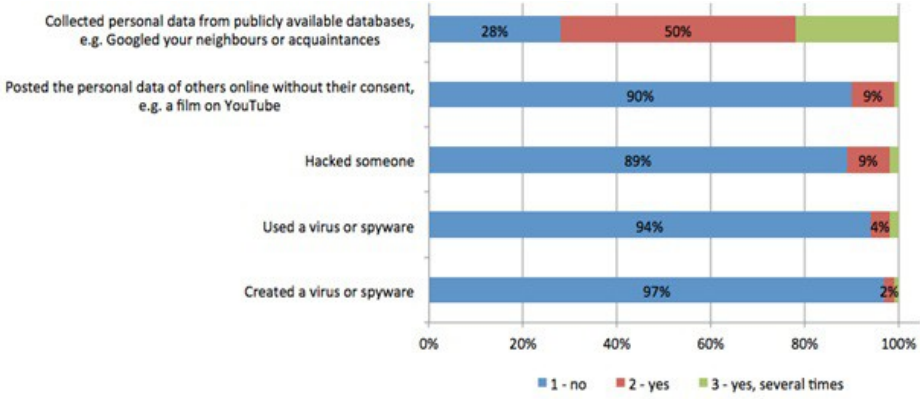


Figure 5: Self-reports on violating the privacy of others

While collecting personal data from publicly available databases is unsurprisingly common – only 28% of the respondents have never Googled other people – the use or creation of malicious code is fairly rare. About one-tenth of the respondents have demonstrated deviant behaviour in social network environments. When the respondents were asked about the types of behaviour that constitute a violation of another person's privacy, we received the following results:

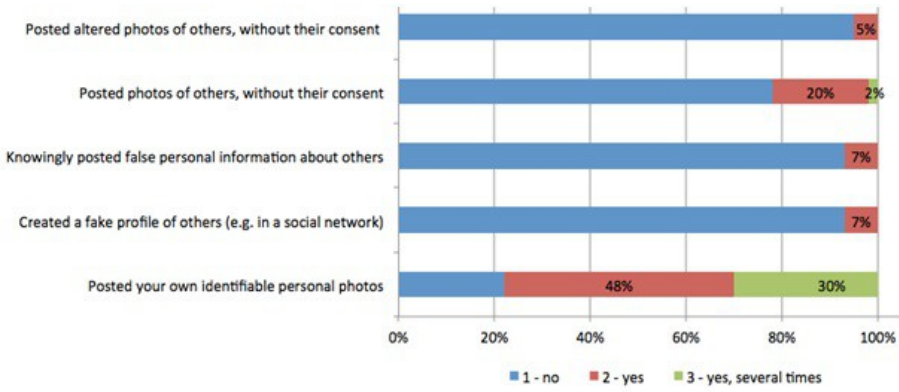


Figure 6: Self-report on violations of another person's privacy on social networks

Publishing photographs without the prior consent of the depicted person ranks as the biggest violation of another person's privacy. Publication of a photograph with the respondent's face clearly visible was performed by 78% of respondents (30% more than once); by comparing the first and second rounds of surveying, we can observe that such posting of photographs increased over time.

5. CONCERN FOR DATA PROTECTION

We asked the respondents about their degree of concern for data protection (sample = n1).

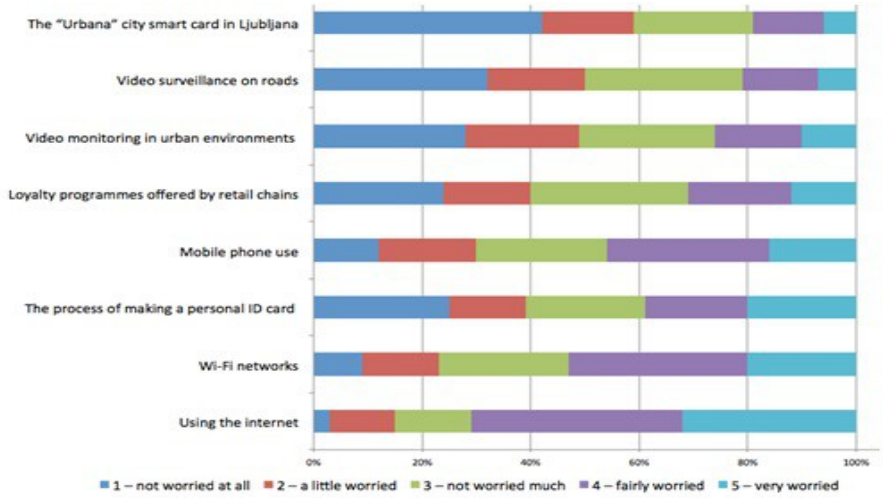


Figure 7: How concerned are you about the protection of your own personal data?

The greatest matter of concern for the respondents appears to be the internet: 70% of the respondents are "quite" or "very" concerned about the internet. Concern also arises as regards being connected to wireless networks (53%) or using mobile telephones (45%). In carrying out a temporal comparison between n1, n2, and n3 we found no statistically significant differences.

How concerned are you about the protection of your own personal data regarding the following matters:	Chi-square	d. f.	P(H0)	Cramer's coefficient
Using the Internet	14.6	4	0.00	0.16
Wi-fi networks	0.0	4	0.30	0.00
The process of making a personal ID card	0.0	4	0.82	0.00
Loyalty programmes offered by retail chains	0.0	4	0.50	0.00
Video surveillance on roads	12.1	4	0.02	0.15
Video monitoring in urban environments	9.7	4	0.05	0.13
While using the "Urbana" city smart card in Ljubljana	0.0	4	0.08	0.00
While using mobile phones	15.7	4	0.00	0.17

Table 1: How concerned are you about the protection of your own personal data regarding the following matters? – gender differences

The results show that gender only slightly impacts concern regarding data protection on the internet (χ^2 = 14.6, p = 0.006), video surveillance on roads (χ^2 = 12.1, p = 0.016) and especially while using mobile phones (χ^2 = 15.7, p = 0.003). The Cramer coefficient also shows a moderate correlation (0.16, 0.15, 0.17, respectively). Women express greater concern in all three variables.

5.1 PERSONAL DATA SAFETY CONCERN REGARDING THE INTERNET

We asked the respondents what their views are on personal data safety while using the internet. There are no statistically significant differences in time or between genders (sample = n2).

Remarkably, one-quarter of the respondents are convinced that they have zero control over data revealed in social networks, despite the fact that almost two-thirds of the respondents set their privacy settings to a "private" mode, and that over two-thirds only communicate online with persons they have known before and in spite of the fact that 80% of the respondents do not share their social network passwords with anyone.

6. HOW RESPONDENTS PERCEIVE THOSE CARRYING OUT SURVEILLANCE

When asked how much certain entities threaten their privacy, the respondents deemed "internet giants" to be the greatest threat, as 56% of the respondents answered "a lot"(4) and "very much" (5) concerning such. Telecom operators came second (25%), and retail chains with "loyalty cards" (23%) third. (Sample = n1).

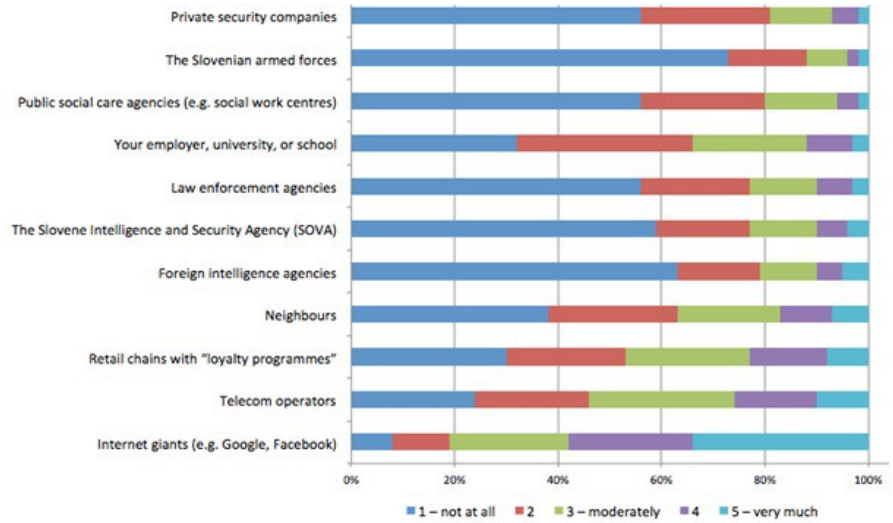


Figure 8: On a scale of 1 to 5, to what degree do you feel the following threaten your privacy?

On a scale of 1 to 5, to what degree do you feel the following threaten your privacy:	Chi-square	d. f.	P(H0)	Cramer's coefficient
Law enforcement agencies	21.5	4	0.00	0.20
Public social care agencies (e.g. social work centres)	3.8	4	0.43	0.08
The Slovenian Intelligence and Security Agency (SOVA)	39.3	4	0.00	0.27
The Slovenian armed forces	18.8	4	0.00	0.19
Foreign intelligence agencies	40.9	4	0.00	0.28
Internet giants (e.g. Google, Facebook)	1.2	4	0.87	0.05
Retail chains with "loyalty programmes"	7.4	4	0.12	0.12
Telecom operators	8.6	4	0.70	0.13
Neighbours	12.4	4	0.15	0.15
Private security companies	21.4	4	0.00	0.20
Your employer, university, or school	3.6	4	0.46	0.08

Table 2: On a scale of 1 to 5, to what degree do you feel the following threaten your privacy? – gender differences

The link between privacy threats and gender is weak for all variables in this category.

Men feel slightly more threatened by foreign intelligence services (χ^2 = 40.9, p = 0.000) and by the Slovenian Intelligence and Security Agency – SOVA (χ^2 = 39.3, p = 0.000). The Cramer coefficient indicates a moderate correlation (0.28 and 0.27, respectively).

By using ordinal logistic regression, we discovered that male respondents respond to this question 0.34 times more with lower ratings (foreign intelligence services) and 0.38 times more with lower ratings when evaluating privacy threats by the Slovenian Intelligence and Security Agency (SOVA); see Figure 9.

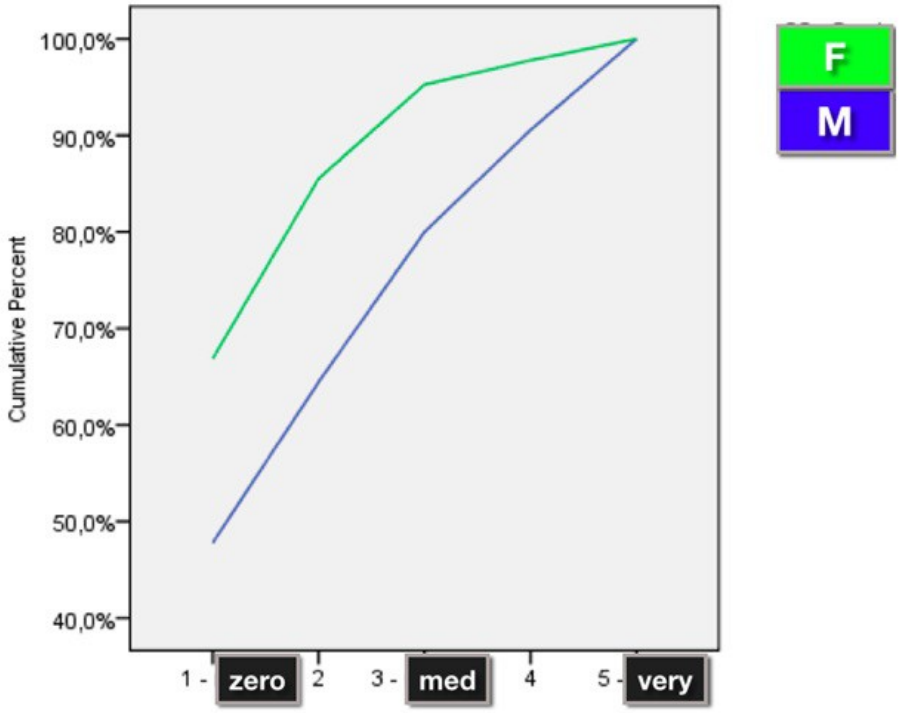


Figure 9: Foreign intelligence services

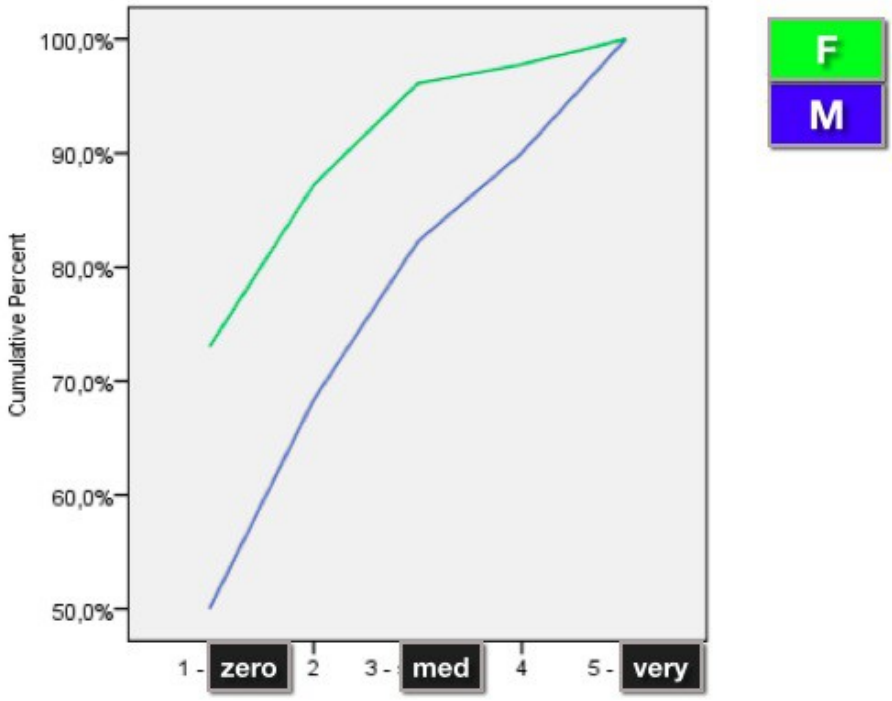


Figure 10: The Slovenian Intelligence and Security Agency – SOVA

A comparison of the responses regarding perceived threats from domestic and foreign intelligence services before and after the Snowden leaks (June 2013) shows that not many people had felt threatened by these intelligence services prior to this event (survey 2012 –2013); a threat level of "zero" was declared by 65% and 60%, respectively, while the same reply in the survey after the affair (September 2013 – January 2014) was only chosen by, respectively, 48 and 44%.

We are able to demonstrate this by comparing the mean (arithmetic middle) and calculating standard deviations: we detected an increase in the mean from 1.67 to 2.14 for foreign intelligence services and an increase from 1.76 to 1.99 for the Slovenian Intelligence and Security Agency.

The standard deviations are similar in both surveys, but they are quite large, which means that the value – an assessment of individual responses – is scattered around the mean.

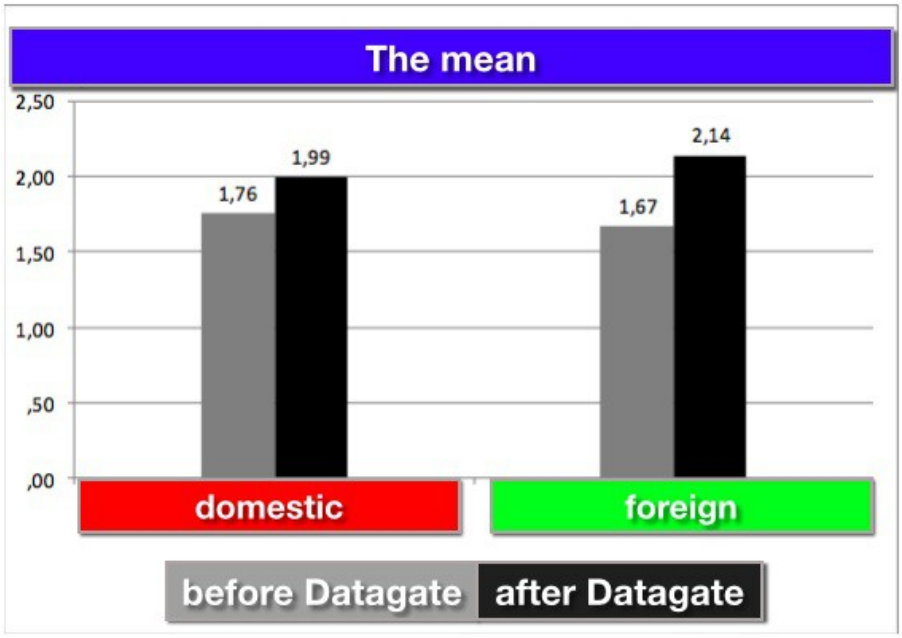


Figure 11: Perceived privacy threats by intelligence services over time – the mean

Standard deviations:

- Slovenian Intelligence and Security Agency SOVA:
  n1 = 1.135, n3 = 1.143;
- Foreign intelligence services: n1 = 1.112, n3 = 1.224.

We detected an increased fear of privacy violations by intelligence services amongst both men and women. For men, the mean increased from 2.09 to 2.48 (foreign intelligence services) and slightly decreased from 2.17 to 2.13 regarding the Slovenian Intelligence and Security Agency (SOVA). However, women have greater fear regarding domestic and foreign intelligence agencies: both values increased, i.e. from 1.46 to 1.91 (foreign intelligence services) and from 1.55 to 1.90 (SOVA).

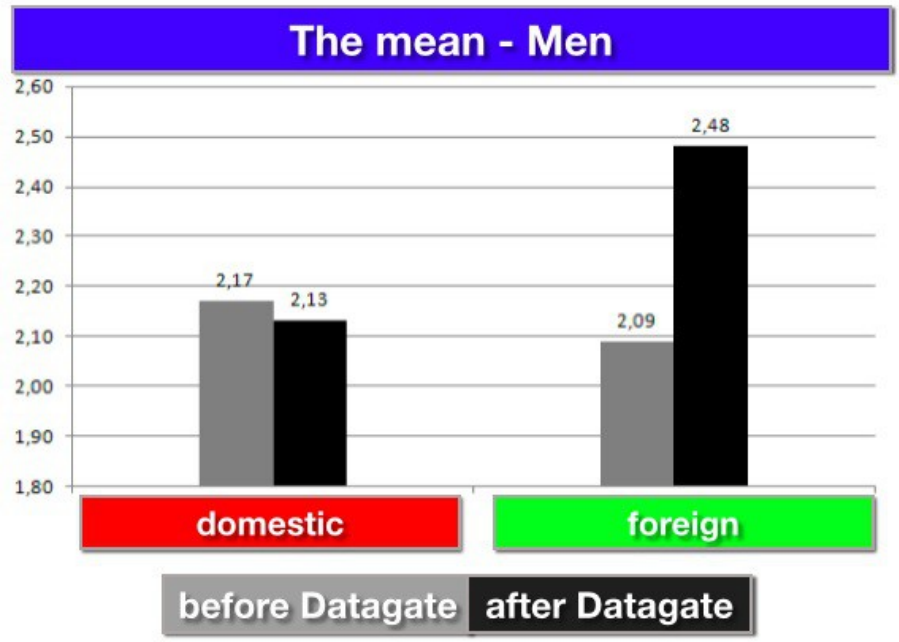


Figure 12: Perceived privacy threats by intelligence services over time (Men) - the mean

The respondents are very well aware of the fact that intelligence agencies around the world do not dispose with the same amount of power. While the US intelligence services exploit the fact that internet giants are American companies regulated to a great extent by the national law, other intelligence services, e.g. those from the Central and East European countries, can not enjoy the benefit of using pressure on such companies. Accordingly, respondents do not perceive domestic intelligence agencies as threatening as foreign intelligence services.

There is also another nationally relevant reason for decrease in Slovenia; and perhaps also in other Central and East European countries. The right-wing governments perceive intelligence services as remnant of the socialist past. These services were constantly under attack after the fall of the Berlin wall of not being enough "democratic". They were also underfunded. The public shaming of the Slovenian intelligence community was far-reaching. Several "political affairs" lead to disclosure of their hidden places and their agents were also compromised. Therefore, national civil intelligence agency is not perceived as a dangerous agency, but as a weak one and not able to conduct huge operations.

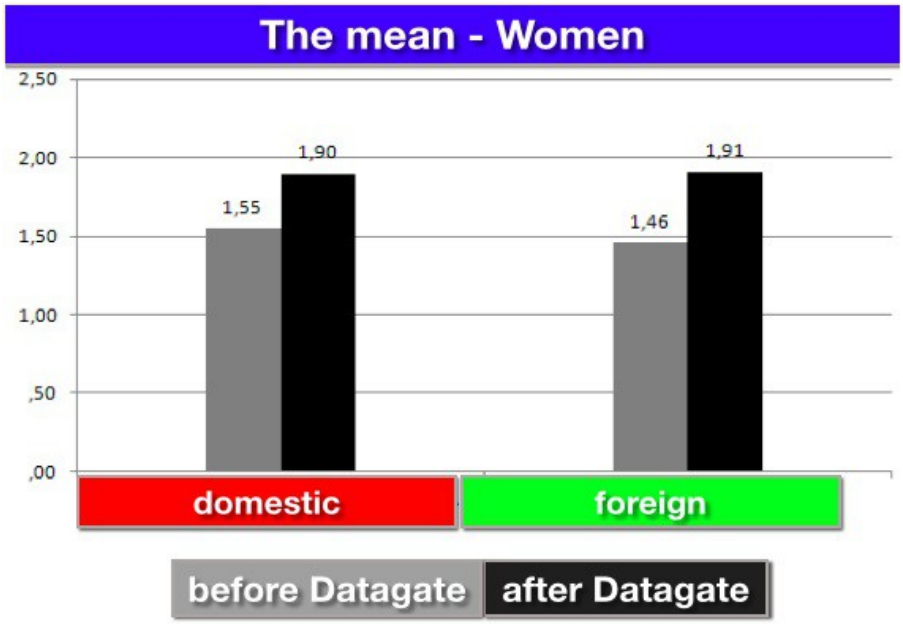


Figure 13: Perceived privacy threats by intelligence services over time (Women) – the mean

7. THE VALUE OF PRIVACY

Respondents are willing to give up their privacy and divulge personal information in exchange for certain benefits. We were interested in how much privacy they are willing to give up. The question we asked them was the following: "Are you willing to submit your personal information (e.g. date of birth, sex, e-mail) in exchange for..." (sample= n1).

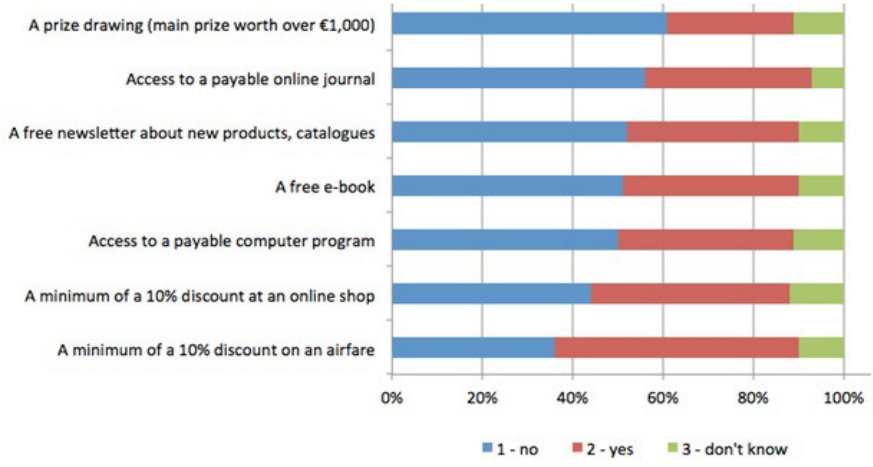


Figure 14: The value of privacy

The respondents felt that entering a prize drawing is the least tempting reason to divulge their personal information: 62% of respondents would not submit their personal information for such a possible benefit. However, the majority of respondents are willing to give up their privacy for at least a 10% discount when purchasing an airline ticket (52%) and many (42%) for at least a 10% discount in an online shop.

When comparing the surveys carried out over time (n1 vs. n3), we only observed a statistically significant difference regarding the option of obtaining "a payable computer program", where the number of respondents who would not submit their personal information for the aforementioned benefit increased (n1 = 51%, n3 = 61%).

Are you willing to submit your personal information (e.g. date of birth, sex, e-mail address) in exchange for:	Chi-square	d. f.	P(H0)	Cramer's coefficient
A free newsletter about new products, catalogues	28.2	2	0.00	0.23
Access to a payable online journal	0.3	2	0.99	0.02
Access to a payable computer program	7.0	2	0.30	0.11
A minimum of a 10% discount at an online shop	0.3	2	0.99	0.02
A minimum of a 10% discount on an airfare	1.7	2	0.42	0.06
A free e-book	13.7	2	0.00	0.16
A prize drawing (main prize over €1,000)	1.9	2	0.38	0.06

Table 3: "Are you willing to submit your personal information (e.g. date of birth, sex, e-mail) in exchange for...?" – gender differences

Gender differences are statistically significant for the option of obtaining "information on products, catalogues, news" (χ^2 = 28.2, sig. = 0.000) and a "free e-book" (χ^2 = 13.7, sig. = 0.001). The Cramer's coefficient indicates a moderate correlation (0.23 and 0.16, respectively). With both variables, men are more reluctant to divulge their personal information.

Finally, we asked respondents about their willingness to support various surveillance technologies on Slovenian roads.

Most respondents support speed cameras on all road sections where there have been fatalities in the last decade (58%). The least popular measure is the installation of traffic light cameras, at 43%. There is no statistically significant gender or temporal difference.

8. VIEWS ON MANDATORY DATA RETENTION REGULATION

Most (53%) of the respondents (sample = n1) were not aware of the provisions of the Slovenian Electronic Communications Act on the mandatory retention of mobile and internet communication traffic data by mobile operators (e.g. information on the persons involved, the time, date, and length of mobile calls, e-mails, visits to certain online addresses, mobile phone location data) for 14 or 8 months.[11] We were curious if, due to the mandatory data retention, respondents tend to decrease mobile or internet communications; the majority, who had previously been informed of the provisions, replied "no" (83%). Similarly, when respondents were asked if they believe that due to data retention other people tend to communicate less with them, only 8% were sure others communicate less.

There is no statistically significant difference between genders.

Furthermore, we asked the respondents if, despite such statutory retention, they were willing to use mobile or internet communication for issues that are of a more personal nature (e.g. communication with a psychotherapist, a lawyer, or a priest): 48% of respondents would use these channels of communication despite the data retention regulation.

Despite the obligatory retention of data, are you willing to use mobile or internet communication for issues that are of a more personal nature (e.g. communication with a psychotherapist, a lawyer, or a priest):	Chi-square	d. f.	P(H0)	Cramer's coefficient
	16.9	10	0.00	0.18

Table 4: Data retention and usage of mobile or internet communication for personal matters – gender differences

The value of the chi-square, and consequently Cramer's coefficient, shows a weak correlation between variables, but is statistically significant. Women tend to take fewer risks when it comes to communicating about personal matters ($\chi^2 = 19.9$, sig. = .000).

[11] Electronic Communications Act (Official Gazette RS, no 109/12, 110/13, 40/14 and 54/14 – ZIN-B).

9. AWARENESS OF PERSONAL DATA PROTECTION REMEDIES

In the last set of questions (sample = n1), we asked the respondents whether and how much they know about the national data protection authority (the Information Commissioner of the Republic of Slovenia – IC). Only 39.5% of the respondents were aware that they can turn to the IC to exercise their right to be informed of their personal data stored or processed by others. 41.6% of the respondents knew that they can turn to the IC when their employer or University installs video surveillance without informing them. A staggering 68.6% did not know that the IC is the authority to turn to when a potential employer demands information regarding family or children. Luckily, awareness seems to be slightly better when confronted with personal data abuse for marketing purposes (e.g. spam), where 45.3% of respondents knew that the IC would be the right entity to turn to for help, while 59.7% of respondents knew that the IC can help in cases of communication eavesdropping.

Are you aware of the possibility to address the Information Commissioner (national data protection authority) in the event of...	Chi-square	d. f.	P(H0)	Cramer's coefficient
A complaint regarding the right to be informed about the collection of your personal data, e.g. by insurance companies or retail chains?	9.9	1	0.00	0.14
A university's/employer's failure to inform you of video monitoring of their premises?	6.9	1	0.01	0.11
Personal data abuse in targeted marketing, e.g. when you receive tailored unwanted e-mail (spam)?	5.2	1	0.02	0.10
Suspicion of communication recording?	0.7	1	0.41	0.04
A potential employer's demand for information regarding family or children?	0.8	1	0.37	0.04

Table 5: Familiarity with the Information Commissioner's work – gender differences

A statistically significant difference exists between the first three questions and gender; the value of the chi-square and Cramer's coefficient is low. Men seem to be better acquainted with the possibility of turning to the Information Commissioner in the event of a violation of privacy.

10. CONCLUSION

The article shows how perception of privacy changes over time and how the awareness of surveillance society has increased because of Snowden's revelations. We feel it is important that citizen are aware of contemporary surveillance practices as these affect their lives significantly not only by denying them their privacy but also leading to "social sorting"[12] and to discrimination. The article shows how awareness of surveillance regimes has increased. This offers a signal for policy makers to reform, e.g. intelligence services, to designing more efficient supervisory mechanisms and increase accountability of those in power.

The online survey results show attitudes towards privacy in various surveillance domains, particularly on the internet and public telecommunications networks and the road surveillance domain. Despite the fact that we asked the respondents about their attitudes towards other surveillance domains and about other data managers and processors, the results show that respondents seem to be mostly worried about the protection of personal data in public telecommunications networks, i.e. when using the internet and mobile phones.

The internet has become an integral part of our lives and it is difficult to find many everyday activities that do not leave a digital trail and/or which are also not connected to public telecommunications networks. That is the reason why the majority of the respondents are concerned about personal data protection on the internet since this is a sphere that does not grant the same degree of privacy as non-digital environments where the possibility of self-protection seems to be greater. In other words, we feel that we are able to control paper money much more than a Bitcoin digital wallet.

Having said that, the cynicism of our respondents is surprising: about one-quarter of the respondents believe that they have zero control over data revealed in social networks, in spite of the relatively high level of self-protection measures used there. This indicates that these measures (e.g. we asked them about privacy settings in social networks, password discretion and sharing passwords with others, exercising prudence in online communications) are easily circumvented, according to the respondents. A imilar, perhaps cynical, attitude can be observed in the consumer

[12] See Lyon, D. 2003, *Surveillance after September 11*, Polity Press, Cambridge.

surveillance domain with regard to loyalty programmes. The respondents quickly "sell" personal data in exchange for a certain benefit. If the respondents gain some profit from their personal data, their reluctance to share such data quickly vanishes.

The respondents are well aware of consumer profiling, segmentation, etc., in the consumer surveillance domain, but due to the overgrowing apathy and resignation (and not naivety), retail chains are highly successful in obtaining their often detailed, and not truly necessary for business, personal data – akin to internet users who do not genuinely believe their personal data is actually protected. Finding themselves in this "wild west" of privacy, they feel it does not matter if they hand over their personal data voluntarily in order to gain at least some benefit from their personal data.[13]

When we examine the answers to the question of who represents the largest threat to privacy, we can observe a growing distrust towards for-profit companies. A solid half of the respondents hold the opinion that online giants (e.g. Google, Facebook) are the main entities carrying out surveillance. In times of crisis, an obvious negative attitude towards such companies that practically "swallow" their users has been growing. Therefore, it is not surprising that we witnessed such views in the survey, where the next biggest threat perceived by respondents comes from telecommunications companies and retail chains with their "loyalty" programmes.

The respondents feel that the fundamental reason for collecting and processing personal data (and consequently threatening privacy) is to profit from others, as they do not benefit whatsoever from submitting this data.

We found the respondents' views on traffic and location data retention performed by telecom operators to be quite casual; 83% do not decrease their internet or mobile communications and 92% of the respondents do not believe that other people tend to communicate less with them due to the above mentioned data retention. One cannot help but wonder what would indeed be a sufficient deterrent to the public's careless use of these communication channels.

Most of the survey was conducted before Edward Snowden leaked NSA documents to the public in June 2013 and before the judgment of the Court of Justice of the European Union (C-293/12 in C-594/12) that declared such

[13] Nocera, J. *The Wild West Of Privacy*. Viewed 7 january 2015. Available at: http://www.nytimes.com/2014/02/25/opinion/nocera- the-wild-west-of-privacy.html?_r=0.

data retention to be disproportionate and lacking appropriate safeguards. With this in mind, it would perhaps be appropriate to repeat the survey.

We were, however, able to verify the influences of Snowden's disclosures with the question on potential threats to privacy by national and foreign intelligence services. The results indicate that the perceived level of threat did indeed increase after June 2013. In our opinion, this can be attributed to Snowden's disclosures, which caused an immense change in people's awareness and broadened the perception of the vast presence, actions, and powers of such intelligence services, all of which generated negative feelings, anger, and fear among the majority of respondents and even deepened distrust towards internet giants and the hidden surveillance state.

Ordinary citizens tend to be "hostages" of traditional as well as distributed powers, which are creating havoc in the digital environment.[14] They have neither the expertise nor means to fend off the rapid and broad authority of both power centres.[15] It seems difficult to prevent surveillance by the state intelligence or to maintain control over our personal data that large corporations in possession of. Similarly, there seems to be little ordinary citizens can do to ward off fraud perpetrated by criminal organizations, who are highly flexible in their use of new information technologies. Accordingly, we seem to live in an "internet feudalism": the feudal lords are googles, amazons, apples, etc., whom we are able to freely choose, in exchange for certain benefits and protection, while we pay for this "security" in a direct or indirect way by submitting our personal data as some sort of feudal currency.[16]

"Privacy" is a concept that changes over time and space, while the law is lagging behind IT development, e.g. the recently unimaginable "privacy in public" is something the law should protect as well. We enter into social relations, which by definition produce a form of control, on an everyday basis. As Lyon (2001) observed, surveillance is a relational concept and so is

---

[14] Schneier, B. *The Battle For Power On The Internet*. Viewed 26 January 2015. Available at: http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/.

[15] Ibidem.

[16] On this subject before Datagate: Schneier, B. *When It Comes To Security, We're Back To Feudalism*. Viewed 12 December 2014. Available at: https://www.schneier.com/essays/archives/2012/11/when_it_comes_to_sec.html.
After Snowden: Schneier, B. *Power In The Age Of The Feudal Internet*. Viewed 2 January 2015. Available at: http:// en.collaboratory.de/w/Power_in_the_Age_of_the_Feudal_Internet.

privacy.[17] It includes the power dynamics and is Janus-faced when it comes to control and care. Similarly, the Slovenian criminologist Pečar (1991) claimed that social control is a double-edged sword: control inevitably occurs every time two individuals meet either in the form of surveillance or care.[18]

Due to the omnipresent nature of contemporary surveillance practices, it is difficult to assess what the processing of massive amounts of personal data (encapsulated in the saying that "data is the new fuel") means for our society. In the future it will be necessary to investigate what our own contribution to such development is and how much we are able to perceive this slippery slope towards the "death of privacy", critically reflect on it and combat the insatiable greed of governments and corporations for our personal data.

LIST OF REFERENCES

BALL, K., & SNIDER, L. (eds.) (2013) *The Surveillance-Industrial Complex: A Political Economy Of Surveillance*. New York: Routledge.

DEN BOER, M., JANSSENS, J., VANDERBEKEN, T., EASTON, M., MOELKER, R. (2010). Epilogue, Concluding Notes On The Convergence Between Military And Police Roles. In EASTON, M., DEN BOER, M., JANSSENS, J., MOELKER, R. & VANDERBEKEN T. (eds.). *Blurring Military And Police Roles*. The Hague: Eleven International Publishing.

DREDGE, S. (2004) Twitter: why #SoggyFries make for a tasty future in big-data revenue. *The Guardian*. [Online] 5th November 2014. Available from: http://www.theguardian.com/technology/2014/nov/05/twitter-soggyfries-big-data-advertising. [Accessed: 15th January 2015].

LUTTERBECK, D. (2005) Blurring The Dividing Line: The Convergence Of Internal And External Security In Western Europe. *European Security*. 14 (2). p.231–253.

[17] Lyon, D. 2001, *Surveillance Society: Monitoring Everyday Life*, Open University Press, Philadelphia.

[18] Pečar, J. 1991, *Neformalno Nadzorstvo: Kriminološki In Sociološki Pogledi*, Didakta, Radovljica.

LYON, D. (2001) *Surveillance Society: Monitoring Everyday Life*. Philadelphia: Open University Press.

LYON, D. (2003) *Surveillance after September 11*. Cambridge: Polity Press.

NISSENBAUM, H. (2004) Privacy As Contextual Integrity. *Washington Law Review*. 79 (1). p.119–158.

NOCERA, J. (2014) The Wild West Of Privacy. *The New York Times*. [Online] 24th February. Available from: http://www.nytimes.com/2014/02/25/opinion/nocera-the-wild-west-of-privacy.html?_r=1. [Accessed: 7th January 2015].

PEČAR, J. (1991) *Neformalno nadzorstvo: kriminološki in sociološki pogledi*. Radovljica: Didakta.

RASHID, F.Y. (2014) Surveillance is the Business Model of the Internet. *Schneier on Security*. [Online] 9th April. Available from: https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html. [Accessed: 14th December 2014].

SCHNEIER, B. (2012) When It Comes To Security, We're Back To Feudalism. *Schneier on Security*. [Online] 26th November. Available from: https://www.schneier.com/essays/archives/2012/11/when_it_comes_to_sec.html. [Accessed: 12th December 2014].

SCHNEIER, B. (2013) The Battle For Power On The Internet. *The Atlantic*. [Online] 24th October. Available from: http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/. [Accessed: 26th January 2015].

SLOVENIA. Electronic Communications Act. *The Official Gazette of the Republic of Slovenia*, no. 109/12, 110/13, 40/14 & 54/14 - ZIN-B.

SOLOVE, D. (2007) "I've Got Nothing To Hide" And Other Misunderstandings Of Privacy. *San Diego Law Review*. [Online] SSRN

Database 44, p. 745. Available from: http://ssrn.com/abstract=998565. [Accessed: 12th August 2015].

VERVAELE, J. (2005) Terrorism And Information Sharing Between The Intelligence And Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law? *Utrecht Law Review*. 1 (1), p. 1–27.

ZAVRŠNIK, A. (2013) Blurring The Line Between Law Enforcement And Intelligence. *Journal of Contemporary European Research*. [Online] 9 (1). p.182–202. Available from: http://www.jcer.net/index.php/jcer/article/view/452. [Accessed: 15th January 2015].