VARSTVOSLOVJE,
Journal of Criminal
Justice and Security,
year 21
no. 4
pp. 333–345

Cyber Landscape of Trust, Fear and Surveillance Concerns: How Slovenians Around the Globe Perceive the Cyberspace

Damjan Fujs, Simon L. R. Vrhovec

Purpose:

The purpose of this paper is to study the differences between countries regarding their residents' trust in government, fear of government intrusions into their privacy and government surveillance concerns in the cyberspace.

Design/Methods/Approach:

A survey has been conducted to capture the perceptions of Slovenians around the globe. Respondents from 58 countries were reached (n = 629) although the results were reported only for countries with at least three respondents. Descriptive statistics were used to describe the sample and measured variables. Graphic illustrations made with MapChart are used to visualize the results.

Findings:

The findings of our study show that perceptions of trust in government, fear of government intrusions into the privacy of country residents and government surveillance concerns vary from country to country. Countries are ranked according to these three criteria. The average trust in government seems to be relatively low. It appears that respondents moderately fear government intrusions into their social network accounts and seem to be concerned about government surveillance over their online activities.

Research Limitations/Implications:

The research contributes to an understanding of the perceptions of Slovenians around the world of trust in government, fear of government intrusions and government surveillance concerns. Although a limited number of countries was reached, the results present some interesting insights into different regions of the world. The study targeted the population of Slovenians around the world thus the readers should be extremely cautious when trying to generalize the results, also due to snowball sampling employed.

Originality/Value:

This paper presents one of the first studies on perceptions of Slovenians around the world regarding their trust in the government of the country of their residence, fear of government intrusions into their privacy and their government surveillance concerns.

UDC: 342.7:004.738.5

Keywords: cyber space, Slovenians abroad, migrant, emigrant, immigrant, expatriate, wiretap, supervision

Kibernetska pokrajina zaupanja, strahu in skrbi glede nadzora: kako Slovenci po svetu dojemajo kibernetski prostor

Namen prispevka:

Namen prispevka je analizirati ključne razlike med državami glede zaupanja v vlado njihovih prebivalcev, njihovega strahu pred vdori države v zasebnost prebivalcev in njihovimi skrbmi zaradi državnega nadzora v kibernetskem prostoru.

Metode:

Da bi zajeli dojemanja Slovencev po svetu, je bila izvedena anketa. Doseženi so bili anketiranci iz 58 držav (n = 629), čeprav so rezultati poročani le za države z vsaj tremi anketiranci. Za opis vzorca in merjenih spremenljivk je bila uporabljena opisna statistika. Grafične ilustracije, narejene s programom MapChart, so bile uporabljene za vizualizacijo rezultatov.

Ugotovitve:

Rezultati raziskave nakazujejo na to, da se dojemanja zaupanja v vlado, strahu pred vdori države v zasebnost njenih prebivalcev in skrbi zaradi državnega nadzora v kibernetskem prostoru od države do države razlikujejo. Države so razvrščene v skupine glede na te tri kriterije. Povprečno zaupanje v vlado se zdi relativno nizko. Zdi se, da se anketiranci srednje močno bojijo vdorov države v njihove račune na družbenih omrežjih in da so zaskrbljeni glede nadzora nad njihovimi aktivnostmi na spletu.

Omejitve/uporabnost raziskave:

Doprinos raziskave je uvid v dojemanje Slovencev po svetu glede zaupanja v vlado, strahu pred vladnim vdorom in strahu pred nadzorom vlade v državi, v kateri živijo. Čeprav smo dosegli omejeno število držav, predstavljajo rezultati nekaj zanimivih vpogledov v različne regije sveta. Študija se je osredotočila na populacijo Slovencev po svetu, zato morajo biti bralci izjemno previdni pri posploševanju rezultatov, tudi zaradi uporabljene metode snežne kepe.

Izvirnost/pomembnost prispevka:

Prispevek predstavlja eno prvih študij dojemanj Slovencev po svetu glede njihovega zaupanja v vlado države, v kateri prebivajo, njihovega strahu pred vdori države v zasebnost njenih prebivalcev in njihove zaskrbljenost zaradi državnega nadzora v kibernetskem prostoru.

UDK: 342.7:004.738.5

Ključne besede: kibernetski prostor, Slovenci po svetu, migrant, emigrant, imigrant, izseljenci, prisluškovanje, nadzor

1 INTRODUCTION

The cyberspace and its services, such as social networks, are connecting people with similar interests and opinions while removing the borders of the physical world thus providing a global place that offers a diverse set of opinions (Bakshy, Messing, & Adamic, 2015). Several cyberspace actors may be active in the cyberspace. For example, some countries may try to use (or misuse) social networks for political and surveillance purposes, for reasons that are either legitimate or not (Stoycheff, 2016). When talking about surveillance in the cyberspace, it may be necessary to distinguish between harmful and harmless surveillance (Trottier, 2011). Harmless surveillance is not inherently harmful to the one being under surveillance and can be performed daily (e.g., checking what someone's friends are doing, commercial surveillance, etc.). However, some authors posit that there is no entirely harmless surveillance (Macnish, 2018). Therefore, it may be better to consider the distinction between those cases that have ethically justifiable reasons for exercising surveillance and those that do not (Huey, 2014; Palm, 2014). Monitoring of cyberspace activities without someone's explicit consent may be against the his or her wishes as it would compromise his or her privacy either way (Humphreys, 2011). Nevertheless, several high-profile examples of state surveillance over citizens surfaced in the past, such as the Snowden disclosures (Johnson, 2017), Iran (Morrison, 2015), Japan (Abe, 2004), China (Wang & Hong, 2010) and various other cases trying to justify surveillance after the 9/11 terrorist attacks on the United States (Michelman, 2009). Surveillance may be done by both, intelligence services which are in the domain of the state and private companies as a form of privatized intelligence (Bures & Carrapico, 2017; Helgesson, 2011).

Trust in the benevolence of cyberspace actors and fear of their surveillance of cyberspace users' online activities may be sensitive factors for cyberspace users that may affect their experience in the cyberspace. Is it possible to trust cyberspace actors that they are working in the best interest of cyberspace users (e.g., tackling terrorism, providing relevant ads) or are they working in their own interests (e.g., tackling political dissent, selling cyberspace users' data for own profits)? Similarly, do cyberspace users fear cyberspace actors and their actions, such as surveillance of their everyday online activities, which may be happening on a large scale according to publicly disclosed information? Social networks may be considered as a honeypot for monitoring and acquiring data given the immense amount of data and their ever-increasing number of users. For example, users post a lot of their personal information, political beliefs and other intimate beliefs on these pages (Semitsu, 2011) which may not be publicly disclosed still present on social networks (e.g., marked as private or posted "only for me"). Currently, social networks play an important role in the political cyber ecosystem as well as a tool for communication and expression of opinion for many politicians, ministers, presidents, activists and others (Zeitzoff, 2017). However, some expressed opinions, such as calls for protests, hate speech and incitement to violence, cannot be considered as positive. Let's highlight just some cases of leveraging social networks for political purposes: Kashmir jihadist recruitment (Kaura, 2017); protest movements in Libya, manipulating public opinion in Russia and Syria, and

paid online commenters in China (Zeitzoff, 2017); protests in Hong Kong (Chan, 2016); Gezi protests in Turkey (Haciyakupoglu & Zhang, 2015); protests in Spain (Hermida & Hernández-Santaolalla, 2018); etc. All these and similar cases may give countries convincing ethical reasons to exercise surveillance over cyberspace users in order to draw up tactics of fighting against protesters and to provide greater security (Zeitzoff, 2017).

In this paper, we focus on the perceptions of cyberspace users regarding the governments of their residing country. Namely, we focus on their trust in government, their fear of government intrusions into the privacy of country residents and their surveillance concerns. In our study, we try to answer our research question:

RQ: Are there differences between countries regarding the perceptions of their residents about trust in government, fear of government intrusions into their privacy and government surveillance concerns?

The aim of this study is to gain an insight into the studied topic, provide possible answers to our research question, and complement existing research on secure and privacy-preserving behavior in the cyberspace (Fujs, Mihelič, & Vrhovec, 2019; Fujs, Vrhovec, & Mihelič, 2018). To achieve this, we developed a research framework and empirically tested it using a survey. We chose the population of Slovenians around the world because they created a new life abroad, were able to adapt well to new living conditions (Celec, 2019; Kuzmič, 2001), and especially because they use information-communication technology in the cyberspace as a tool to communicate with those who are not spatially close to them (Milharčič Hladnik, 2008). To conform to the widely accepted definition of Slovenians around the world, the study includes immigrants, namely people who are working abroad but return to Slovenia daily.

The rest of the paper is organized as follows. In Section 2, we describe the research methods used. In Section 3, we present the main results of our study. Finally, we discuss the results in Section 4 and present some concluding remarks in Section 5.

2 METHOD

We conducted an online survey among Slovenians around the world. The survey was advertised via private contacts and business contacts of researchers, through mailing lists and groups on social platforms, such as Facebook. Snowball sampling (i.e., respondents were asked to further advertise the survey among their peers) was employed to maximize the reach of the survey. Due to the sensitivity of the topic, respondents were informed before taking the survey that their participation in the research is voluntary and that the collected data will be used only for research purposes. They were also informed that there were no right or wrong answers to the questions, and that they could stop filling in the questionnaire at any time. The questionnaire was available in Slovenian and English. A total of 629 responses were received from February to June 2019. 39.3 percent of respondents were male, 59.8 percent were female, and the rest did not disclose their gender. The age of respondents ranged from 16 to 110 years (M = 41.49, SD = 15.92).

Respondents were generally well-educated as 14.1 percent had competed high school or less, 33.5 percent had completed a Bachelor's degree (first cycle), 36.4 percent finished their Master's (second cycle) and 14.5 percent obtained a PhD (third cycle). Most respondents were active as 12.9 percent were students, 67.6 percent employed, 5.7 percent unemployed and 11.9 percent retired.

The questionnaire consisted of 3 constructs measuring trust in government (TiG), fear of government intrusions into privacy (FoGI) and government surveillance concerns (GSC). Each construct was measured with three items that were adopted from previous studies: TiG (Harrison McKnight, Choudhury, & Kacmar, 2002), FoGI (Osman, Barrios, Osman, Schneekloth, & Troutman, 1994) and GSC (Nam, 2018). Respondents were asked to rate the items using a five-point Likert scale ranging from 1 (*Strongly Disagree*) to 5 (*Strongly Agree*). IBM SPSS Statistics version 26 and Microsoft Excel were used to perform statistical analyses of the results. The reliability of the constructs was evaluated by calculating the Cronbach's alpha (CA) coefficient. CA values above 0.80 indicate good *reliability*. Items of construct with adequate reliability were aggregated into new construct variables on which subsequent analyses were conducted.

3 RESULTS

In this section, we first summarize the results of descriptive statistics analysis. Then, we provide the visual presentation of the results.

Table 1 presents the descriptive statistics for all 9 variables measured in the survey. Descriptive statistics and Cronbach's alpha for constructs were also calculated. At the beginning it is worth mentioning that this is aggregated data of respondents from several countries and does not represent any single country.

Table 1: Descriptive statistics for aggregated constructs

Code	Construct	*M*	*SD*	*CA*
TiG	Trust in government	2.61	0.97	.881
FoGI	Fear of government intrusions	3.00	1.13	.904
GSC	Government surveillance concerns	3.16	1.15	.952

M = mean, *SD* = standard deviation, *CA* = Cronbach's alpha

We analyzed each construct across countries where the respondents resided. Results of analysis for only 36 countries are presented as we excluded all countries that were represented with less than 3 respondents to avoid a bias due to a low number of respondents. First, averages for each country were calculated. Next, countries were ordered according to their mean values for each construct. The first third of all countries were assigned a *Low* rank, the second third were assigned the rank *Medium*, and the rest were ranked as *High*. Table 2 presents the boundary mean values for ranks of individual constructs.

Table 2: Boundary mean values for ranks of individual constructs

Rank	*TiG*	*FoGI*	*GSC*
Low	1.515 – 2.415	1.833 – 2.741	1.667 – 2.915
Medium	2.578 – 2.865	2.743 – 3.076	2.933 – 3.290
High	2.866 – 3.833	3.198 – 3.933	3.333 – 4.300

TiG = Trust in government, *FoGI* = Fear of government intrusions, *GSC* = Government surveillance concerns

The results of country rankings are shown in Table 3.

Table 3: Country rankings according to mean scores of individual constructs

Country	*TiG*	*FoGI*	*GSC*
Argentina	Low	Low	Medium
Australia	Medium	Medium	High
Austria	Medium	Medium	Medium
Belgium	High	Low	Low
Bosnia and Herzegovina	Medium	High	High
Brazil	High	Medium	Medium
Canada	Medium	High	High
China	Low	High	High
Croatia	Low	High	High
Czechia	Low	Medium	High
Finland	High	Low	Low
France	Medium	Medium	Medium
Germany	Medium	Low	Medium
Greece	Low	High	Low
Hungary	Low	High	High
Ireland	High	Low	Medium
Italy	Medium	Medium	High
Luxembourg	High	Low	Low
Montenegro	High	Medium	Low
Netherlands	High	Low	Medium
New Zealand	High	Low	Low
North Macedonia	Medium	High	High
Norway	High	Low	Low
Poland	Low	High	High
Portugal	Medium	Low	Low
Serbia	Low	High	High
Slovakia	Low	High	Low
Slovenia	Low	Medium	Medium
Spain	Medium	Medium	Medium
Sweden	High	Medium	Low
Switzerland	High	Medium	Medium
UK	Medium	Low	Low
US	Low	High	Medium

TiG = Trust in government, *FoGI* = Fear of government intrusions, *GSC* = Government surveillance concerns

To make it easier for readers to comprehend the results of our study, we visualized them by creating a figure of ranked countries for each construct. Included countries are colored with different shades of gray. A darker shade means a higher mean score for the country. Namely, light gray, dark gray and

black represent *low*, *medium* and *high* rank, respectively. Countries not covered by our study due to not having enough respondents and thus not being included in our analyses are colored white.

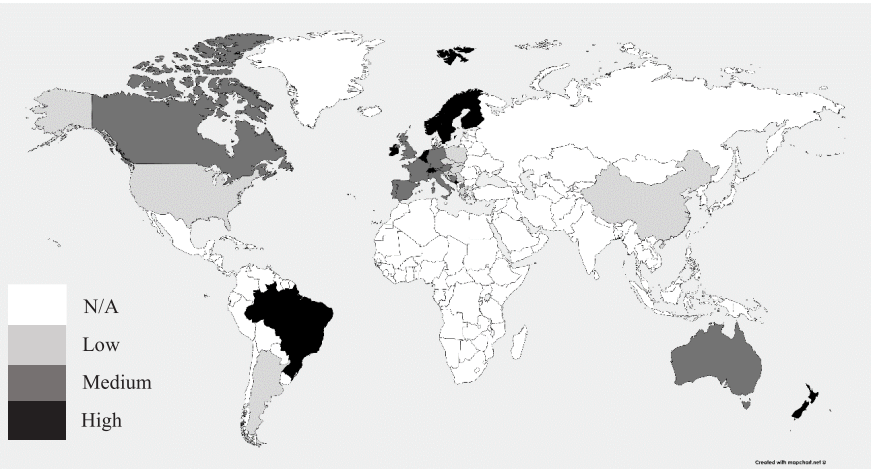


Figure 1: Distribution of the perceptions regarding respondents' trust in government (TiG)

Figure 1 shows the country ranks according to perceived trust in government of respondents. Slovenians around the world appear to trust especially some governments of Northern, Central and Western European countries (i.e., Belgium, Finland, Ireland, Luxembourg, Netherlands, Norway, Sweden and Switzerland). Additionally, Montenegro, Brazil and New Zealand, are completing this club. Trust in governments seems to be relatively low for countries in Eastern Europe and the Balkans (i.e., Croatia, Czechia, Greece, Hungary, Poland, Serbia, Slovakia and Slovenia), China, Argentina and US.

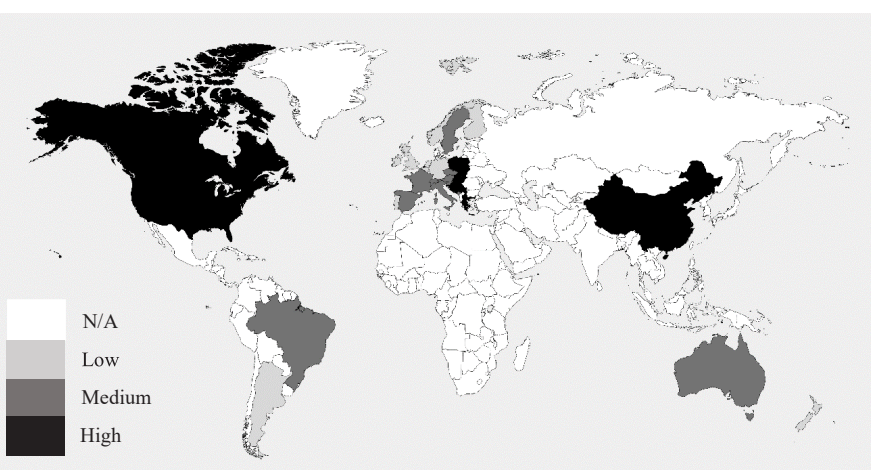
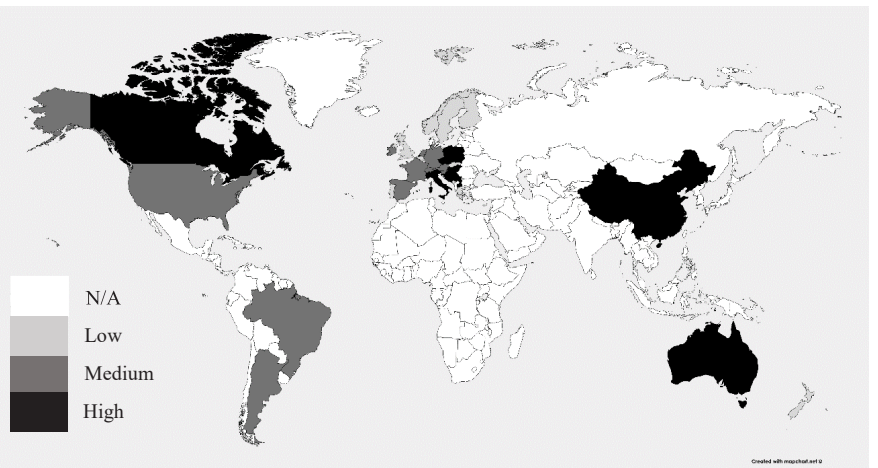


Figure 2: Distribution of the perceptions regarding respondents' fear of government intrusions into their privacy (FoGI)

As can be seen in Figure 2, fear of government intrusions into privacy is especially present in Eastern Europe and the Balkans (i.e., Bosnia and Herzegovina, Croatia, Greece, Hungary, North Macedonia, Poland, Serbia and Slovakia), Africa (i.e., Sierra Leone), China and North America (i.e., Canada and US). Complementary

to our findings regarding trust in governments, fear of government intrusions is relatively low in several countries in Northern, Central and Western Europe (i.e., Belgium, Finland, Germany, Luxembourg, Netherlands, Norway, Portugal and UK), Argentina and New Zealand.

Figure 3: Distribution of government surveillance concerns of the respondents (GSC)



Government surveillance concerns of respondents are shown in Figure 3. Countries with high surveillance concerns can be found in Eastern Europe and the Balkans (i.e., Bosnia and Herzegovina, Croatia, Czechia, Hungary, North Macedonia, Poland and Serbia), Italy, Canada, Australia and China. Surveillance concerns appear to be low mostly in various countries in Europe (i.e., Belgium, Finland, Greece, Luxembourg, Montenegro, Norway, Portugal, Slovakia, Sweden and UK). Only respondents in New Zealand have comparably low surveillance concerns in studied countries outside of Europe.

4 DISCUSSION

A brief view at the mean values gives an interesting overview over the perceptions of the respondents. First, the average trust in government seems to be relatively low (i.e., below the middle value 3 on a 5-point scale). Second, it appears that respondents moderately fear government intrusions into their social network accounts which may be a consequence of well-known leaks about government activities described above. Cyberspace users may therefore perceive governments as surveillance actors with notable capabilities. Third, people seem to be concerned about government surveillance over their online activities. This paper has several theoretical and practical implications discussed in the next subsections.

4.1 Theoretical Implications

Countries often measure trust in the government as form of mining public opinion. Trust of immigrants in government may however differ from the trust shown by locals. Trust in government may be an indication of the government policy on

immigrants or a sign of widespread dissatisfaction with the elected politicians who rule the country. The results of our study suggest that trust in government of countries with right-wing political options (e.g., Hungary, Poland, Serbia, USA, Slovakia and Croatia) is low which may be related to their anti-immigrant policies and/or propaganda. Trust in government may be also related to income, life expectancy and life satisfaction in general. For example, trust in governments of countries that have among the highest incomes and life expectancy (e.g., Ireland, Finland, Belgium, Switzerland, Luxembourg, Norway, Netherlands, New Zealand and Sweden) is high. Nevertheless, some other countries, such as Brazil and Montenegro, with a high level of trust somewhat stand out and future work would be needed to determine if there really is an association between these factors (Gapminder Foundation, 2019).

A quick glimpse at the world map of fear quickly suggests that the fear of government intrusions may be high at the border between East and West, namely in Eastern Europe and the Balkans. On one hand, fear may be a legacy of the iron curtain without proper justification. On the other hand, such fear may be aroused due to the perceived motivation of some European governments to monitor their citizens for security reasons. For similar reasons, China, Canada and US may also be highly motivated. A sufficiently motivated and resourceful country may be able to develop or otherwise acquire (e.g., by buying spyware) the means needed to eavesdrop on their residents and especially immigrants. Future qualitative studies (e.g., interviews) may be highly beneficial to gain a deeper understanding of the factors leading to high levels of government intrusions in these countries.

One might expect there to be a high level of fear of government intrusions when the level of trust in a government is low. Some cases appear to confirm this hunch (i.e., China, Croatia, Greece, Hungary, Poland, Serbia, Slovakia and US). China is one of the largest countries in the world by population and is known to have a powerful apparatus, resources and puts a lot of effort into surveilling its people. Similarly, US is also known to have vast surveillance resources and similarly to some European countries low trust in governments may be a consequence of a right-wing anti-immigrant government. Nevertheless, we observed that Argentina has both low trust in government and low fear of government intrusions diametrically contrary to such common sense-making. Simply put, residents in Argentina do not appear to trust their governments however they are also not afraid of these governments' intrusions into their privacy. This may be explained by a perceived lack of governments' capabilities or motivation (or both) for intruding the privacy of residents in these countries.

Finally, we also studied respondents' concerns regarding government surveillance online (e.g., emails, social networks, searching and browsing habits). Surveillance concerns appear to be high in similar regions as fear of government intrusions is high although they do not appear to be always aligned. Government fear may be more related to the perceived motivation of governments to monitor the residents. Surveillance concerns may however incorporate the capability and willingness of the governments to monitor residents in practice. For example, fear of government intrusions into privacy are relatively high while surveillance concerns seem to be quite low in Greece and Slovakia. Slovenian immigrants there

do not appear to be too concerned about government surveillance although their fear of government intrusions is high. Either they do not perceive the government capable of doing such monitoring or they simply think that the probability of such an event is very low even though the government is able to surveil them. To better understand the discrepancies between fear of government intrusions and surveillance concerns, more research using qualitative methods would be needed.

An interesting question stemming from results on surveillance concerns arises. Do surveillance concerns affect the adoption and use of technology? Although we cannot give a definitive answer, we can try to provide some insights for the readers. The use of certain technologies is forbidden in some countries. For example, it is forbidden to use social networks, such as Facebook, in China. In Turkey, it is forbidden to use Wikipedia, and in Saudi Arabia, it is forbidden to use WhatsApp, Skype and SnapChat among others. The use of end-to-end encrypted communication is also frequently forbidden (e.g., Telegram in Iran and Russia). We can therefore safely assume that use of technology depends on the country of residence. This may not appear to be related to surveillance concerns. However, surveillance concerns may be high in such countries. Even though it may affect the use of certain types of technology, it may not affect the use of different technologies in general. If cyberspace users cannot use Facebook, they may simply use VK.

4.2 Practical Implications

The data we have obtained through this body of research allow us to draw some practical implications. First, the results emphasized that there are different levels of perception (from low to high) regarding government activity in the cyberspace. This indicates that people should protect themselves against surveillance (e.g., by using encrypted communication, adequately secured wireless networks, secure applications) in countries where surveillance concerns are higher and government trust is lower to feel more comfortable in the cyberspace. This may hold even more when communicating with their friends and family outside of the country of residence as governments might be interested in monitoring these connections more closely.

Next, the same measures may be used by Slovenians living in Slovenia when communicating with their friends and family abroad. Especially when sharing sensitive data with residents of countries where government fear is high, trust in government is low, or surveillance concerns are high.

Finally, the identified differences between countries suggest that residents and visitors to different countries around the world would benefit from some advisory on this topic. The Ministry of Foreign affairs may include a cyber landscape assessment and recommended countermeasures in their advisory for Slovenians living or travelling to different countries around the globe. This may be however a sensitive diplomatic issue especially if a government would like to keep a low profile over their activities in the cyberspace. Therefore, non-governmental organizations may help to complement the official channels.

4.3 Limitations

This paper has some limitations the readers should note. First, we have uneven population patterns across countries. It would be highly beneficial to improve the samples for underrepresented countries. Second, we reached a limited number of different countries in our study. Future studies providing insight into other countries would offer a more holistic view of the research subject. Third, snowball sampling was employed thus caution is needed when generalizing its results.

5 CONCLUSION

Our study provided some important insights into how Slovenians around the world perceive the governments in the countries where they currently reside and their concerns regarding those governments' surveillance. The results of our study enable us to answer our research question positively. Not only there are differences between countries regarding the perceptions of their residents about trust in government, fear of government intrusions into their privacy and government surveillance concerns, but there appear to be differences regarding the relations between these three constructs depending on the country. As one of the first studies on perceptions of Slovenians around the world regarding their trust in the government of the country of their residence, fear of government intrusions into their privacy and their government surveillance concerns, the study seems to open more new questions than it answers calling for more research on the topic. First, how does the type of the political regime affect trust, fear and surveillance concerns. Second, does the regulation of human rights and known government interventions (e.g., mass surveillance) affect these constructs. Third, how much does being a minority and feeling a different legal treatment influence these same constructs. Finally, does the media coverage of high-profile cases of data misuse, surveillance technologies, loss of privacy, etc. impact the perceptions of cyberspace users regarding their trust in government, their fear of government intrusions and their government surveillance concerns.

REFERENCES

Abe, K. (2004). Everyday policing in Japan: Surveillance, media, government and public opinion. *International Sociology*, *19*(2), 215–231. doi:10.1177/0268580904042901

Bakshy, E., Messing, S., & Adamic, L. A. (2015). Exposure to ideologically diverse news and opinion on Facebook. *Science*, *348*(6239), 1130–1132. doi:10.1126/science.aaa1160

Bures, O., & Carrapico, H. (2017). Private security beyond private military and security companies: Exploring diversity within private-public collaborations and its consequences for security governance. *Crime, Law and Social Change*, *67*(3), 229–243. doi:10.1007/s10611-016-9651-5

Celec, Š. (2019). *Slovenci v Betlehemu 2* [Slovenes in Bethlehem 2]. Retrieved from https://www.youtube.com/watch?v=16K_gn0bzow&t=499s

Chan, M. (2016). Social network sites and political engagement: Exploring the impact of Facebook connections and uses on political protest and participation. *Mass Communication and Society*, *19*(4), 430–451. doi:10.1080/15205436.2016.1161803

Fujs, D., Mihelič, A., & Vrhovec, S. (2019). Social network self-protection model: What motivates users to self-protect? *Journal of Cyber Security and Mobility*, *8*(4), 467–492. doi:10.13052/jcsm2245-1439.844

Fujs, D., Vrhovec, S., & Mihelič, A. (2018). What drives the motivation to self-protect on social networks? The role of privacy concerns and perceived threats. In S. Vrhovec (Ed.), *Proceedings of the Central European Cybersecurity Conference 2018 on - CECC 2018* (pp. 1–6). New York: ACM Press. doi:10.1145/3277570.3277581

Gapminder Foundation. (2019). *Gapminder: Free vizualization tool*. Retrieved from https://www.gapminder.org

Haciyakupoglu, G., & Zhang, W. (2015). Social media and trust during the Gezi protests in Turkey. *Journal of Computer-Mediated Communication*, *20*(4), 450–466. doi:10.1111/jcc4.12121

Harrison McKnight, D., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *The Journal of Strategic Information Systems*, *11*(3–4), 297–323. doi:10.1016/S0963-8687(02)00020-3

Helgesson, K. S. (2011). Public-private partners against crime: Governance, surveillance and the limits of corporate accountability. *Surveillance & Society*, *8*(4), 471–484. doi:10.24908/ss.v8i4.4183

Hermida, A., & Hernández-Santaolalla, V. (2018). Twitter and video activism as tools for counter-surveillance: The case of social protests in Spain. *Information Communication and Society*, *21*(3), 416–433. doi:10.1080/1369118X.2017.1284880

Huey, L. (2014). The problem with ethics: Difficulties in constructing normative frameworks. *Surveillance and Society*, *12*(1), 140–141. doi:10.24908/ss.v12i1.5194

Humphreys, L. (2011). Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication*, *61*(4), 575–595. doi:10.1111/j.1460-2466.2011.01570.x

Johnson, C. N. (2017). A "massive and unprecedented intrusion": A comparative analysis of American journalistic discourse surrounding three government surveillance scandals. *Digital Journalism*, *5*(3), 318–333. doi:10.1080/21670811.2016.1251330

Kaura, V. (2017). Countering insurgency in Kashmir: The cyber dimension. *ORF Ocassional Paper*, *32*(January), 1–23.

Kuzmič, M. (2001). *Slovenski izseljenci iz Prekmurja v Bethlehemu v ZDA 1893-1924: Naselitev in njihove zgodovinske, socialne, politične, literarne in verske dejavnosti* [Slovenian emigrants from Prekmurje in Bethlehem, Pennsylvania, USA, 1893–1924]. Ljubljana: Založba ZRC, ZRC SAZU.

Macnish, K. (2018). *The ethics of surveillance: An introduction*. Abingdon: Routledge.

Michelman, S. (2009). Who can sue over government surveillance? *UCLA Law Review*, *57*(1), 71–114.

Milharčič Hladnik, M. (2008). Internet in preobrazbe ohranjanja kulturne dediščine v slovenskoameriških etničnih skupnostih [Internet and the transformations in preserving cultural heritage in American-Slovenian ethnic communities]. *Dve Domovini / Two Homelands*, (28), 57–71.

Morrison, E. (2015). Surveillance society needs performance theory and arts practice. *International Journal of Performance Arts and Digital Media*, *11*(2), 125–130. doi:10.1080/14794713.2015.1084812

Nam, T. (2018). Untangling the relationship between surveillance concerns and acceptability. *International Journal of Information Management*, *38*(1), 262–269. doi:10.1016/j.ijinfomgt.2017.10.007

Osman, A., Barrios, F. X., Osman, J. R., Schneekloth, R., & Troutman, J. A. (1994). The pain anxiety symptoms scale: Psychometric properties in a community sample. *Journal of Behavioral Medicine*, *17*(5), 511–522. doi:10.1007/BF01857923

Palm, E. (2014). Conditions under which surveillance may be ethically justifiable: Remarks on Kevin Macnish's proposed normative theory of surveillance. *Surveillance and Society*, *12*(1), 164–170.

Semitsu, J. (2011). From Facebook to mug shot: How the dearth of social networking privacy rights revolutionized online government surveillance. *Pace Law Review*, *31*(1), 291–381.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effect in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly*, *93*(2), 296–311. doi:10.1177/1077699016630255

Trottier, D. (2011). A research agenda for social media surveillance. *Fast Capitalism*, *8*(1), 59–68. doi:10.32855/fcapital.201101.008

Wang, S. S., & Hong, J. (2010). Discourse behind the forbidden realm: Internet surveillance and its implications on China's blogosphere. *Telematics and Informatics*, *27*(1), 67–78. doi:10.1016/j.tele.2009.03.004

Zeitzoff, T. (2017). How social media is changing conflict. *Journal of Conflict Resolution*, *61*(9), 1970–1991. doi:10.1177/0022002717721392

About the Authors:

Damjan Fujs, received his BSc degree in Information Security in 2017, MA degree in Criminal Justice and Security, both at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. Currently he is a Member of Information Systems Laboratory, Teaching Assistant and Doctoral Candidate at Faculty of Computer and Information Science, University of Ljubljana, Slovenia. E-mail: damjan.fujs@fri.uni-lj.si

Simon L. R. Vrhovec, PhD, is an Assistant Professor at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. He received his PhD degree in Computer and Information Science from the University of Ljubljana in 2015. E-mail: simon.vrhovec@um.si