Jelena Budak Institute of Economics, Zagreb
jbudak@eizg.hr

November 28, 2018

Behavioural consequences of privacy violation online in a post-communist society: resilience explained?

Introduction

The phenomena of privacy resilience is still an underexplored issue for many reasons. There is an ongoing debate on concepts and definitions, and there is a lack of theoretical approaches as well as of empirical studies of privacy resilience.

The aim of this paper is to shed light to privacy perceptions and attitudes of internet users, in a specific context of ex-communist society. The research is conducted on the population of internet users to tackle one of the core questions regarding privacy today: if and how privacy as a system can adapt and survive in a digital age. Is there any privacy left on the internet? Fast changes, rapid development and the increasing possibilities of information and communication technologies make that in developed countries practically every segment of our life is somehow *online*.

Privacy and resilience are hot issues in ICT field. IT security has to ensure the resilience of the system against loss of personal data and other information, in parallel with safeguarding the privacy of information by for example, blocking an unacceptable access to the data (Crowcroft, 2015). A definition from the practitioner point of view is offered by Raymund E. Liboro, Chairman of National Privacy Commission (Philipinnes, 2017): ‘Applied to privacy, resilience simply means always being aware of threats and risks, being one step ahead, and having processes in place that will

allow one to respond—quickly, efficiently, and in a manner that minimizes further damage. An entity is privacy resilient when it is able to prevent privacy risks from coming to fruition.'[1] In this sector, organizations make efforts to develop an effective resiliency plan against disruption caused by security risks.

However, the debate on privacy and resilience is evolving across disciplines. An environmental economist Neil Adger says that 'Resilience is fundamentally an interdisciplinary concept that requires both the natural and social sciences'.[2]

The research on privacy and resilience certainly has its applicative value in everyday life. For example, resilience of surveillance and privacy in the smart cities might be enhanced because of the risk management and regulations behind their use (and not misuse); at least citizens believe these mechanisms do protect them efficiently (Hiller and Blanke, 2017).

The notion of resilience in social research is explained and different definitions offered by Raab, Jones and Szekely (2015). The authors illustrate at the example of public goods the distinction between the concepts of "resistance" and "resilience". They describe different outcomes of reactions to shocks in the course of time: resistance prevents deviations from the ideal state so no recovery is needed while resilience helps to recover after stress. There are two possible outcomes of resilience: full recovery, which is the return to the previous ideal state, and partial recovery whereas the real state after recovery is not equal to the ideal state before the shock.

The academic discussion should evolve about the notion and manifestations of resilience of privacy and privacy resilience. Although in

1 https://business.mb.com.ph/2017/10/19/privacy-resilience/
2 https://www.stockholmresilience.org/research/research-videos/2008-05-28-how-can-we-apply-social-sciences-to-the-resilience-concept.html

different languages the term resilience has no straightforward meaning[3], the issue is much more complex than in pure semantic sense. Here we offer simple distinctive explanations. Resilience of privacy is denoting our individual or society or 'system' capability to preserve privacy. Privacy resilience might be understood as how privacy as a system recovers and adapts after being lost by privacy intrusion. The personal privacy resilience is intuitively hard to be (re)established if an individual experienced privacy breaches. The same stand for societies that have lived in the authoritarian regimes under surveillance and with limited privacy. For example post-communist societies are expected to be more prone to privacy concerns and less tolerant to the contemporary surveillance (see for example Webster et al. Eds, 2011; Svenonius and Björklund, 2018).

In the privacy resilience research, the recovery to the 'normal' state of privacy from the individual point of view is effectuated by personal actions. The knowledge on factors influencing privacy resilience and how to measure it is very limited, if any. This study contributes to the privacy resilience debate by exploring how individual behaviour relates to the privacy restored after stress. The research is done in the online environment because in the digital age, the meaning of privacy has evolved and nowadays it focuses on personal information shared with family, friends, businesses, and strangers, while consumers must actively participate in self-protection as new digital technologies represent potential threat to their privacy (Markos et al., 2012). Behavioural consequences in the online environment are far more complex than in offline environment (Ginosar and Ariel, 2017). Furthermore, post-communist societies due to the past regime might be more sensitive to privacy intrusions. Previous study for Croatia showed that citizens who are mostly concerned about data and privacy protection belong to the part of national population of employed citizens with higher education and income

3 For example in Croatian language, resilience is depending on the context, translated as resistance, recovery or elasticity.

(Budak et al., 2013) yet according to our best knowledge there is no research on privacy resilience in post-communist countries.

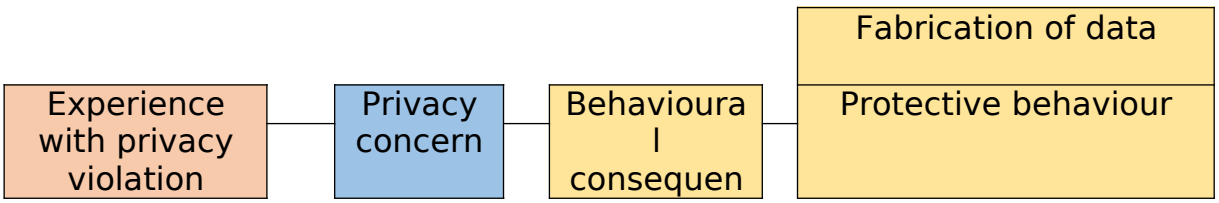
In the exploratory study conducted on the large sample of internet users in Croatia, we provide some insights how past negative privacy violation experience of internet user is related to privacy concern and what actions could be foreseen in the case of individuals that have been exposed to the privacy breach and those who have not experienced privacy violation.

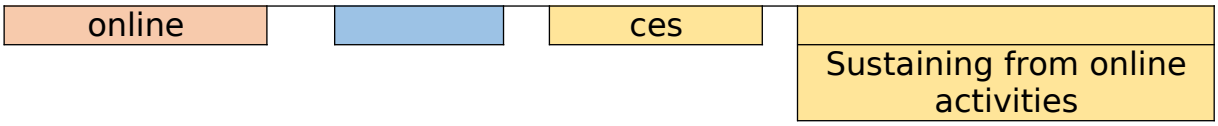
Model

Experience with privacy violation online is expected to increase individual concern about privacy protection and possible future (mis)use of private data and personal information. The level of privacy concern is a subjective category and rather difficult to be measured. In our survey the scales were taken from the existing literature (Smith, Milberg & Burke, 1996) measuring individual's concern for privacy and applied to measure internet users' information privacy concerns (Malhotra, Kim & Agarwal, 2004). The methodology of adapting the borrowed pre-tested scales from the literature to measure privacy concerns in the online environment is explained in detail in Anić et al. (2018).

Negative past experience with privacy violation might raise the privacy concern of internet users and lead to the behavioural consequences: fabrication of data, protective actions, and sustaining from online activities, as presented in the conceptual model for this research (Figure 1).

Figure 1: Conceptual model





Behavioural consequences are measured by three variables adopted from Wirtz, Lwin & Williams (2007). They consist of fabrication of personal information, sustaining from giving out personal information and using tools for actively protecting one's privacy. The expected consequence of an increased online privacy concern is altered protective behaviour in the form of withholding information, providing false information or protection of information including technical protection (e.g. software installed). Lwin et al. (2007) stated that reactive behaviour implies personal information fabrication, withholding and protecting by using privacy enhancing technologies. Another behavioural reaction to an increased online privacy concern is less online usage in the future, including refrain from surfing on the Internet or limiting the range of online activities. People concerned about their privacy when online might change their intention to adopt new online services or technologies. More concerned users might decide not to make online purchases, or e-banking transactions. Some concerned people might refrain from social networks or even from using smartphones.

Methodology and data

In order to explore the relations presented in Figure 1., we use the survey data on the internet users population in Croatia. Survey data were collected by Computer-Assisted Telephone Interviewing (CATI) method during a period of November 2015 to March 2016 within the PRICON project[4] (as described in Anić et al., 2018). Internet users in Croatia represent the population for this study, and secondary data were used (Stilus Media) to assess the number of Internet users in Croatia. Online phone book was used as a sampling frame. The sample was made on a one-way stratification by 21 counties. The sample allocated to each

4 This work has been fully supported by the Croatian Science Foundation under the project number 7913.

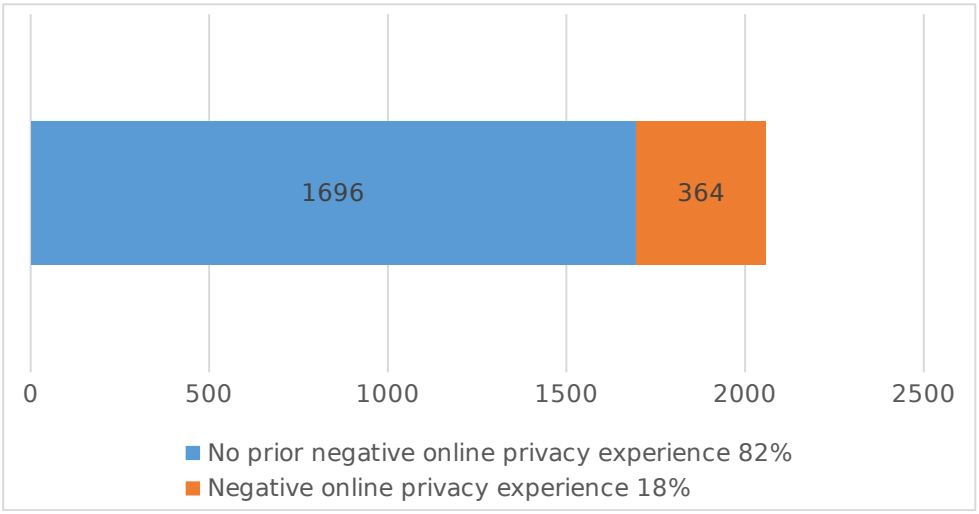
stratum was proportional to the assessed number of internet users each stratum. Within each stratum a combination of random and systematic sampling was applied. Pages from phone book were selected using simple random sampling procedure. Sample units within each page were selected applying systematic sampling procedure. The final sample consists of 2,060 Internet users aged 18 or older. Of the large questionnaire and the whole survey dataset, in this study we use the selected questions to measure variables in the model, as listed in Appendix.

The measurement instrument used in this study includes one yes or no question regarding past (negative) experience, and fifteen questionnaire items on privacy concern and behavior online. Except for the past experience, each item in the questionnaire was measured by a Likert-type five-point scale, ranging from 1 (strongly disagree, absolutely no) to 5 (strongly agree, absolutely yes). Next we provide the description of results.

Results

The vast majority of internet users in Croatia (82 %) claimed they had not experienced any privacy violations on the internet (Figure 2). The 18 percent of internet users who had experienced privacy violation on the internet, or have witnessed this happened to a close person are in the focus of our interest. This is the part of the internet population whose privacy had been exposed to stress and we believe that analysis of their actions and opinions could shed more light to the privacy resilience.

Figure 2. Internet users and their experience with privacy violation on the Internet, n=2060

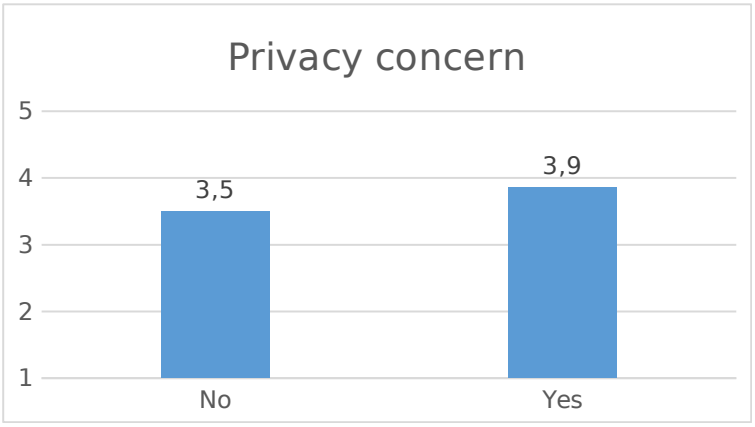


Source: Survey data.

In the following section, we will investigate the correlation between the prior negative experience of privacy intrusions online and different attitudinal and behavioral consequences of internet users.

Internet users who had prior privacy violation experience have expressed higher levels of privacy concern online (Figure 3). As expected, prior negative experience with privacy breaches increases the privacy concerns. However, that part of internet population might have not been concerned before the privacy violation stress, and that event might have increased dramatically the level of privacy concern online. Here we observe the ex-post concern only so the statistically significant difference of about ten percent in privacy concern score is not so evident as one might expect. Both groups of respondents on average showed relatively low levels of privacy concern online.

Figure 3. Prior privacy violation experience and privacy concern



Note: t= -7.256; df=574.90, p-value=0.000

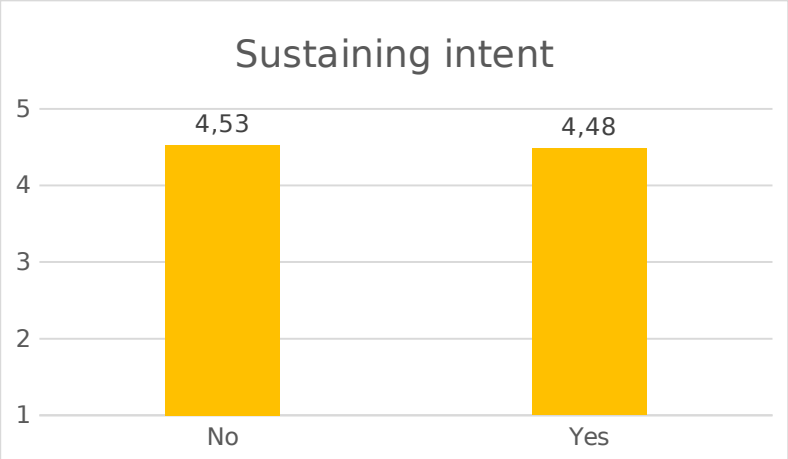
Source: Survey data.

It would be sound to assume that internet users behave accordingly to their experiences and concerns and that bad memory evoke behaviour that is more defensive. However, this assumption is not evidenced by the survey data analysis. Figure 4 clearly shows that the sustaining behavior is widespread among Internet users in Croatia, no matter of privacy violation experience. All respondents claim they regularly refuse to provide personal data, often leave the untrustworthy web site or avoid registering online (an average grade for both users with and without bad privacy experience is around 4.5 on the scale 1-5). Interestingly, intentions to sustain from giving information are slightly stronger among users who had no bad experience with privacy intrusions before although the difference is not statistically significant. Plausible explanation is that sustaining actions and privacy concern nexus is two-fold. Internet users who are very cautious when online are therefore less exposed to privacy breaches and have less privacy violation experience. In our model sustaining intent is considered as a result of privacy concern, yet one could think of sustaining intent as an antecedent of privacy concern as well.

Expressed sustaining intentions of Internet users in Croatia indicate they would easily refrain or withdraw from online activity. An average internet user in Croatia intents to sustain from giving information almost every time when performing some activity online. At much lesser extent, they

would employ more specific protection actions allowing them to stay online and to preserve privacy at the same time.

Figure 4. Prior privacy violation experience and intent to sustain from giving information

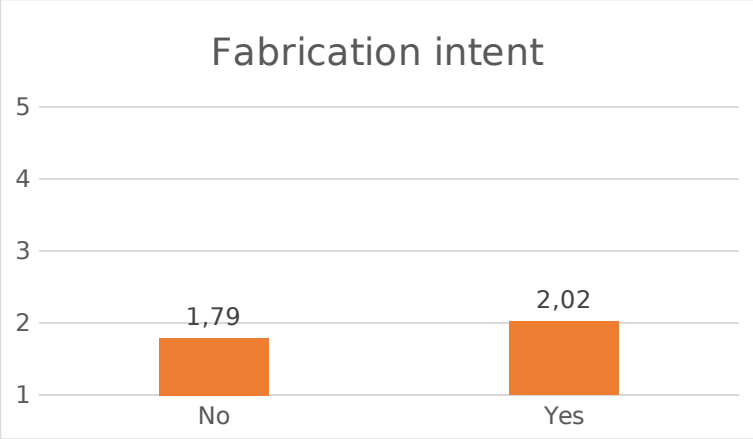


Note: t = 1.098; df = 542.85; p-value = 0.273.

Source: Survey data.

Internet users in Croatia almost never give false information or fabricate personal data and this practice is, as expected slightly more spread among users that have experienced privacy violations (Figure 5).

Figure 5. Prior privacy violation experience and intent to fabricate information online

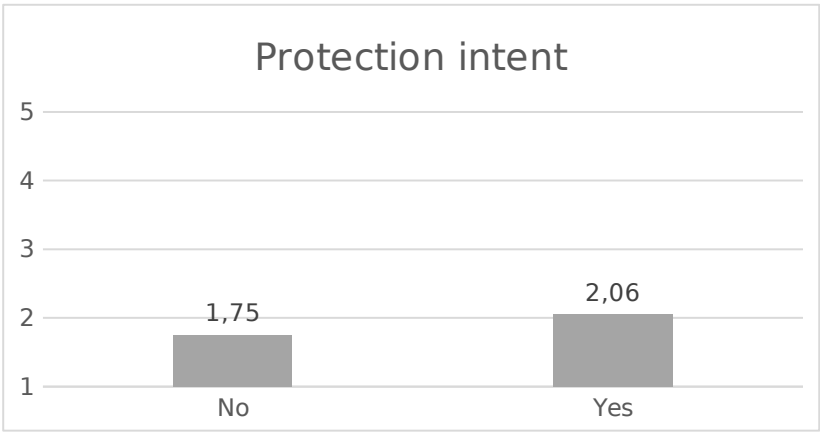


Note: t = -3.628; df = 498.95; p-value = 0.000

Source: Survey data.

The intent to install software that allows private browsing and use of similar tools that preserve privacy when online is more evident for internet users who had experience with privacy violation (Figure 6), although as in the previous case of fabrication, this practice is almost never applied by an average internet user in Croatia.

Figure 6. Prior privacy violation experience and protection behavior



Note: t = -4.435; df = 488.67; p-value = 0.000

Source: Survey data.

Conclusion remarks

Internet users in Croatia who have been exposed to privacy violation or at least have heard of that bad experience from persons close to them, are more privacy concerned and behave more cautiously when online. However, the differences in their behaviour when compared to the majority of internet users who had no prior negative experience with privacy breaches are rather small. In the context of further research needed there are indications of *resilience of privacy* because privacy concerns in general are only slightly present (mean score of 3.5 and 3.9 at the scale 1 to 5). As far as it considers *privacy resilience* first insights into behaviour of internet users who have been exposed to stress of privacy violation suggest they easily ‘adapt’ and recover i.e. no major behaviour

reactions are taken when compared to the internet users whose privacy had not been stressed. The analysis we provide has its limitations. One of the limitations is we do not examine causal relationships.

Finally, although Budak and Rajh (2018) suggest that privacy concern might be taken as a proxy for surveillance concern, privacy might be employed as a tool for resilience against surveillance and its effects in the digital era. In this sense, privacy resilience evolves beyond just preserving individual subjective notion of privacy despite intrusions.

Acknowledgments

Thanks to Vedran Recher for useful comments.

References:

Anić, I. D., Budak, J., Rajh, E., Recher, V., Škare, V., Škrinjarić, B., & Žokalj, M. (2018). The Extended Model of Online Privacy Concern. Zagreb: Ekonomski institut, Zagreb.

Budak, J., Rajh, E. (2018), Citizens' Online Surveillance Concerns in a Post-Communist Country. *Surveillance & Society* 16 (13), 347-361.

Budak, J., Anić, I-D., Rajh, E. (2013), Public attitudes towards privacy and surveillance in Croatia. *Innovation – The European Journal of Social Science Research*, special issue Technology and Privacy, 26 (1-2), 100-118.

Crowcroft, J. (2015), On the duality of resilience and privacy. *Proceedings Royal Society A*, 471: 20140862. http://dx.doi.org/10.1098/rspa.2014.0862

Ginosar, A. and Ariel, Y. (2017), "An analytical framework for online privacy research: what is

missing?", *Information & Management*, 54(7), 948-957.

Hiller J.S., and Blanke, J.M. (2017), Smart Cities, Big Data, and the Resilience of Privacy. *Hastings Law Journal*, 68(2), 309-56.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 35(4), 572-585.

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale and a causal model. *Information System Research*, 15(4), 336-355.

Markos, E., Labrecque, L.I & Milne, G.R. (2012). Web 2.0 and consumers' digital footprint: managing privacy and disclosure choices in social media. In Close A.G. (Ed.), Online consumer behaviour: theory and research in social media, advertising, and e-tail (pp. 157-182). New York: Routledge.

Raab, C. D., Jones, R., and Szekely, I. (2015), Surveillance and Resilience in Theory and Practice (August 17, 2015). *Media and Communication*, 3(2), 21-41. http://dx.doi.org/10.17645/mac.v3i2.220

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring, Individuals' Concerns about Organisational Practices. *MIS Quarterly*, 20(2), 167-196.

Svenonius, O., Björklund, F. (2018). Explaining attitudes to secret surveillance in post-communist societies. *East European Politics*, 34 (2), 123-151.

Webster, W., Balahur, D., Zurawski, N., Boersma, K., Sagvari, B., Backman, C. eds., Living in Surveillance Societies: The Ghosts of Surveillance, Proceedings of LiSS Conference 2, Iasi: Editura Universitatii "Al. I. Cuza", 2011.

Wirtz, J., Lwin, M., & Williams, J. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, 18(4), 326-348

Appendix: Selected items of the questionnaire, N=2060

NEGATIVE EXPERIENCE

Have you or somebody close to you have had bad experiences with regard to privacy violation on the internet before?	Yes	No

To what extent do you agree with the following statements? 1- strongly disagree, 2- disagree, 3-neither agree or disagree, 4-agree, 5- strongly agree

PRIVACY CONCERN

I am concerned about my online privacy.
All things considered, the Internet would cause serious privacy problems.
Compared to others, I am more sensitive about the way my personal information is handled online.
I am concerned about extensive collection of my personal information over the Internet.
I am concerned about my privacy violation when using the internet.
Compared with other subjects on my mind, personal privacy online is very important.

How often do you behave in the following ways when on the Internet? 1- never, 2-almost never, 3-sometimes, 4-almost every time, 5-every time

FABRICATION

I give fictitious responses to avoid giving the web site real information about myself.
I use another name or e-mail address when registering with certain web site without divulging my real identity.

PROTECTION

I use software so that the recipient cannot track the origin of my mail.
I use software to eliminate cookies that track my Internet activities.
I use software to disguise my identity.

SUSTAINING

I am reluctant to register with my personal information to the websites I don’t completely trust.
I refuse to provide personal information to untrustworthy websites.
I avoid visiting the untrustworthy websites.
I don’t purchase goods from untrustworthy websites.