Razvoj i zabrinutost za online privatnost u zemljama zapadnog Balkana: pogled odozgo

Recher, Vedran; Budak, Jelena; Rajh, Edo

Source / Izvornik: **Radni materijali EIZ-a, 2015, 5 - 23**

Journal article, Published version
Rad u časopisu, Objavljena verzija rada (izdavačev PDF)

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:213:766620

Vedran Recher, Jelena Budak and Edo Rajh

Eye in the Sky: Contextualizing Development with Online Privacy Concern in Western Balkan Countries

Srpanj . July 2015

Radni materijali EIZ-a . EIZ Working Papers

HR EXCELLENCE IN RESEARCH

ekonomski institut, zagreb

Br . No EIZ-WP-1502

Radni materijali EIZ-a
EIZ Working Papers
EIZ-WP-1502

Eye in the Sky: Contextualizing Development with Online Privacy Concern in Western Balkan Countries

Vedran Recher
Doctoral Researcher
The Institute of Economics, Zagreb
Trg J. F. Kennedyja 7
10000 Zagreb, Croatia
T. 385 1 2362267
F. 385 1 2335165
E. vrecher@eizg.hr

Jelena Budak
Senior Research Associate
The Institute of Economics, Zagreb
Trg J. F. Kennedyja 7
10000 Zagreb, Croatia
T. 385 1 2362228
F. 385 1 2335165
E. jbudak@eizg.hr

and

Edo Rajh
Senior Research Associate
The Institute of Economics, Zagreb
Trg J. F. Kennedyja 7
10000 Zagreb, Croatia
T. 385 1 2362298; F. 385 1 2335165
E. erajh@eizg.hr

www.eizg.hr

Zagreb, July 2015

IZDAVAČ / PUBLISHER:
Ekonomski institut, Zagreb / The Institute of Economics, Zagreb
Trg J. F. Kennedyja 7
10000 Zagreb
Croatia
T. 385 1 2362 200
F. 385 1 2335 165
E. eizagreb@eizg.hr
www.eizg.hr

ZA IZDAVAČA / FOR THE PUBLISHER:
Dubravka Jurlina Alibegović, ravnateljica / director

GLAVNI UREDNIK / EDITOR:
Ivan-Damir Anić

LEKTURA / LANGUAGE EDITING:
Doris Baničević

IZVRŠNA UREDNICA / EXECUTIVE EDITOR:
Marijana Pasarić

Tiskano u 80 primjeraka
Printed in 80 copies

ISSN 1846-4238
e-ISSN 1847-7844

Contents

Eye in the Sky: Contextualizing Development with Online Privacy Concern in Western Balkan Countries

Abstract

The online privacy issue has received a great deal of scholarly attention in the past decade. Studies for Western developed societies have shown that privacy concern and risk awareness are higher in more developed countries; however, the relevance of *online* privacy concern in the context of economic development remains unexplored. In a digital society, online privacy concern could have significant impact on the real economy; therefore it is not to be underestimated. If indeed development is influenced by the penetration of new technologies, the connection between online privacy concern and development could have a major role in post-transition economies. In this paper we try to determine the level of online privacy concern in a set of post-transition, Western Balkan countries and its repercussions on the future development of these countries. Past research for the Western Balkan region has shown significant structural differences in general privacy concern and here we introduce a new approach which focuses on online privacy concern. We contextualize online privacy with the implementation of reforms which are crucial for the Western Balkan region as well as for other less developed and post-transition economies. The differences in the level of online privacy concern among post-transition Western Balkan countries are discussed in the context of their economic, technological and institutional development, and policy implications are suggested.

Keywords: online privacy concern, development, Western Balkans
JEL classification: D18, M15, O39

Razvoj i zabrinutost za *online* privatnost u zemljama zapadnog Balkana: pogled odozgo

Sažetak

Problem zabrinutosti za *online* privatnost dobio je značajnu pozornost istraživača u proteklom desetljeću. Istraživanja za zapadna razvijena društva pokazala su da su zabrinutost za privatnost te poimanje rizika viši u razvijenim zemljama. Međutim, relevantnost zabrinutosti za *online* privatnost u kontekstu ekonomskog razvoja ostaje neistražena. U digitalnom društvu zabrinutost za *online* privatnost može imati snažan učinak na realnu ekonomiju i ne smije se podcijeniti. Ako doista postoji veza između razvoja i zabrinutosti za *online* privatnost, razvoj u posttranzicijskom razdoblju bit će pod značajnim utjecajem penetracije novih tehnologija. U ovom radu pokušavamo odrediti razinu zabrinutosti za *online* privatnost u odabranim posttranzicijskim zemljama zapadnog Balkana te reperkusije na budući razvoj tih zemalja. Prethodna istraživanja za regiju pokazala su značajne strukturne razlike u općoj zabrinutosti za privatnost, a ovdje se uvodi novi pristup koji se fokusira na zabrinutost za *online* privatnost. *Online* privatnost promatra se u kontekstu provedbe ključnih reformi za regiju zapadnog Balkana, kao i za ostale manje razvijene posttranzicijske zemlje. Razlike u razini zabrinutosti za *online* privatnost između posttranzicijskih zemalja zapadnog Balkana razmatraju se u kontekstu njihovog ekonomskog, tehnološkog i institucionalnog razvoja, zajedno s implikacijama za nositelje javnih politika.

Ključne riječi: zabrinutost za *online* privatnost, razvoj, zapadni Balkan
JEL klasifikacija: D18, M15, O39

1 Introduction*

Online privacy has received a great deal of scholarly attention in the past decade. Studies for Western developed societies have shown that privacy concern and risk awareness are higher in more developed countries. This is not a surprising result, but is in line with Maslow's hierarchy of needs (Maslow, 1943); when basic needs are fulfilled, only then people tend to care about their privacy, which is the case in more developed countries. Therefore, it is important to realize the relevance of online privacy concern in the context of economic development, which is currently an unexplored area of the online privacy concern discourse. If there is indeed a connection between online privacy concern and economic development as we expect, it is undoubtedly a subtle and indirect one. However, in a digital society, online privacy concern could have sufficient impact on the real economy not to be underestimated. Privacy concern in an online environment is important for the implementation of reforms (e.g., e-government), and for enhancing the business climate (e.g., social networks, online stores, information gathering). Proper management of online privacy concern might facilitate creating successful business policies (e.g., marketing strategies), and could benefit national security and political stability. In this paper we aim to determine the level of online privacy concern in Western Balkan countries and its repercussions on the future development of these countries.

Past research for the Western Balkan region (Budak, Rajh, & Anić, 2015) has shown significant structural differences in privacy concern in everyday life based on age, education, employment and country of origin. This research introduces novelties in the model; we use a more contemporary approach which focuses on *online* privacy concern. This area of research is represented in the US and gaining importance in the European context, but to the best of our knowledge there are no studies focused on post-transition economies. Our intuition is that economic development in the post-transition era will be majorly influenced by the penetration of digital technologies. Furthermore, we contextualize online privacy with the implementation of reforms which are crucial for the Western Balkan region as well as for other less developed and post-transition economies, and we inspect this issue with regards to improving the business climate and supporting economic development.

* This work was supported by Croatian Science Foundation under the project 7913.

We have conducted a large survey in Bosnia and Herzegovina, Croatia, FYR of Macedonia and Serbia with over 2,000 respondents forming nationally representative samples for four countries in the region. The large general population data enabled an empirical analysis of attitudes and behaviors of citizens related to privacy concern in the Western Balkans. We have examined the level of online privacy concern and its determinants in terms of gender, age, education and the country of origin, controlled by internet usage, and constructed the PRICON (PRIvacy CONcern) index, measuring the level of people's concern for privacy when acting online. The differences in the level of online privacy concern among post-transition Western Balkan countries are discussed in the context of their economic, technological and institutional development.

The paper is structured as follows. The next section is a literature overview of privacy and online privacy concern and findings relevant for the privacy and development nexus and for our set of countries. The third section describes the institutional set-up as defined by the European Union (EU) accession process and its importance for privacy. Methodology and data are explained in chapter four, and the results are discussed in section five. The last section concludes.

2 Literature Overview

There is a growing literature on online privacy; however, the impact of online privacy concern on different aspects of offline life remains somewhat esoteric. As Reed (2014) notes, being online today goes beyond internet usage. Therefore, it is important to comprehend the intertwinement between online privacy concern and its economic consequences in the real world. In this paper we will contextualize internet penetration and online privacy concern with economic development. Obviously, before conducting an analysis it is important to perceive the complex notion of privacy in general.

Alan Westin provided one of the most cited definitions of privacy: "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1970). In a modern society, privacy is recognized as an individual right, but also as a social and political value (Raab & Goold, 2011; Solove, 2008a; Goold, 2010). Solove (2008a) argues that in a modern society

"the value of privacy must be determined on the basis of its importance to society, not in terms of individual rights". Fuchs (2011) also emphasizes this important distinction and argues that the question is not how privacy can be best protected, but in which cases whose privacy should be protected and in which cases it should not be protected. The dominant approach to privacy in the literature is that privacy is related to individual rights to protect one's self, from the state and organizations and from other individuals. The other approach sees privacy as a social value: common good, public value, collective value (Regan, 1995; Fuchs, 2011), and a political value.

Flaherty (1989) emphasizes the distinction between privacy and data protection. He argues that "privacy" is a broad and all-encompassing concept that contains a whole host of human concerns about various forms of intrusive behavior, including wiretapping, surreptitious, physical surveillance and mail interception. On the other hand, "data protection" is a form of privacy protection that is involved with control of the collection, use and dissemination of personal information. Therefore, data protection is implemented to limit this type of surveillance by third persons and thus to preserve individual privacy. It is at present the most critical component of privacy protection, because of the ongoing automation of databases. Solove (2008b) exhibits a pyramid concept of data abuse and argues that abuse of personal information is ubiquitous in the digital age, but not due to technology but due to government and business practices. At the top of the pyramid is the misuse of personal information in obviously harmful ways. In the middle of the pyramid are leaks of personal information from the company or organization databases. At the bottom of the pyramid is insecurity on how well the data are protected. In this study we are interested in people's concern about these intrusive behaviors. Moreover, we examine the antecedents of online privacy concern and observe its interaction with economic, institutional and technological development.

Previous studies indicate that there are differences in information privacy concerns across cultures (Dinev et al. 2005; Ur & Wang, 2013), and that different groups of people share different views on surveillance and privacy (Haggerty & Gazso 2005; Wirtz et al. 2007). Citizens' attitudes towards privacy and data protection also vary according to demographic characteristics (e.g., European Commission, 2011). Wirtz et al. (2007) indicate that citizens who show less concern for (internet) privacy are those individuals who perceive that corporations are acting responsibly in terms of their privacy policies and that sufficient legal regulation is in place to protect their privacy, and have greater trust and confidence in these

power-holders. On the other hand, if those in power positions (regulators and firms) are not seen to be responsible, consumer concern is likely to increase, and thus could lead to defensive measures to reduce the level of dependence on these power-holders.

The spread of new technologies and global communications has raised the issue of privacy when acting online. Privacy concern in the everyday life of people and organizations is strongly associated with their presence in the cyber world, and indeed online privacy concern is in the focus of contemporary research.

Based on their survey and analysis, Buchanan et al. (2007) suggest three scales for measuring the level of online privacy concern: a general one, called "privacy concern", which is defined through people's attitude towards privacy, and two behavioral ones, "general caution" and "technical protection", related to people's demeanor with regards to protection of their privacy. However, our focus is on the general scale of online privacy concern, since it is well documented in the literature that people's privacy concern is rarely related to behavior focused on actually protecting their privacy (see for example Acquisti, 2004; Acquisti & Grossklags, 2007).

Although no study has explicitly examined the relationship between the level of economic development and online privacy concern *per se*, from most of the studies examining online risk awareness and online privacy concern it is implicitly clear that more developed countries have a higher level of online privacy concern. For example, Warren & Brandeis (1890) describe the development of new privacy laws resulting from political, social and economic changes that entail the recognition of new rights. Wang, Norcie & Cranor (2011) find that American social network users are the most privacy concerned, followed by the Chinese and Indians; which is also in line with their level of economic development. Additionally, it is intuitive that this relationship holds without empirical proof for at least two reasons: (i) less developed societies have limited access to broadband internet (Reed, 2014), (ii) based on Maslow's hierarchy of needs (Maslow, 1943), it is hard to expect significant privacy concern in undeveloped economies where basic human needs are not met. Furthermore, as Goold (2010) notes, the state must also recognize that privacy has an important role to play in the promotion of democracy and other fundamental human rights such as freedom of expression and freedom of association, which often go hand-in-hand with economic development.

The channels through which the relationship between development and online privacy concern operates are well documented in the literature, but are rarely explicitly stated as such. For example, Belanger, Hiller & Smith (2002) stress that winning public trust is the primary hurdle to continued growth in e-commerce, and Liu et al. (2004) state that concerns regarding privacy and trust are potential obstacles to growth and represent important issues to both individuals and organizations. Furthermore, companies realize that protecting the private information of their consumers is an essential component in winning their trust (McKnight & Chervany, 2001). Moreover, privacy concerns often present obstacles to the adoption of new technologies and services (Sheng, Nah, & Siau, 2008).

Studies exploring privacy concern in developing countries and in particular for post-transition economies are scarce. Past research of general privacy concern in Western Balkan countries has shown that demographic characteristics as well as the country of origin stand as significant determinants of privacy concern (Budak, Rajh, & Anić, 2015). Anić, Rajh, & Budak, (2014) find for a set of Western Balkan countries that EU membership is positively related to privacy concern in general.

In line with the views stated above, we further contextualize online privacy concern in Western Balkan countries with their EU accession path as a main determinant of their future evolution to developed economies.

3 EU Accession Path and Privacy

To a large extent, the EU accession process determines the objectives and pace of economic policies, reforms and supportive regulation in acceding countries. By signing the Stabilization and Association Agreement (SAA), one of the first steps of the accession process, the harmonization of national legislation with the EU *acquis communautaire* begins. During the negotiation process that follows for candidate countries, the European Commission carefully monitors national progress in implementation of recommended policies. The Western Balkan countries observed in this research are on different milestones along the EU membership path. Croatia is an EU member state as of July 1, 2013. Two candidate countries are FYR of Macedonia and Serbia. FYR of Macedonia was granted the candidate country status in

December 2005 and the accession negotiations opened in October 2009. Serbia was granted the EU candidate country status later, i.e., in March 2012 and the formal start of Serbia's accession negotiations was in January 2014. Bosnia and Herzegovina has still a long way ahead to EU membership. Bosnia and Herzegovina was identified as a potential candidate in June 2003, and the SAA signed in 2008 has been ratified but has not yet entered into force (European Commission, 2015).

Differences in the path to the EU might have a crucial role because, as David Lipton, IMF First Deputy Managing Director, wrote in the foreword of the IMF publication on 15 years of economic transition in the Western Balkans, "perhaps the most tangible achievement of all lies in the fact that most of the Western Balkan countries are on a path towards European Union accession" (International Monetary Fund, 2015:5). We argue that EU accession is relevant to contextualizing privacy for a set of reasons, first of all because of EU regulations implemented in the course of the accession.

In the EU in general, data protection and fundamental safeguarding of privacy rights of EU citizens are of great importance, and a majority of EU citizens show concern about their privacy and data protection (European Commission, 2011), which indicates that people are aware of potential risks of sharing data. O'Mahony & Flaherty (2009) analyze the EU legal framework for consumer protection and conclude that many deficiencies and shortcomings still exist. The reason behind this is the extremely fast-changing online environment and the inability of regulations to follow its advancements.

EU privacy directives stem from the European Convention on Human Rights defining a right to the respect for private and family life (European Court of Human Rights, 2015).[1] For a summary of the European privacy policy and a list of the most relevant policy documents from 2000 onwards within international organizations, the European Union, selected member states and the US related to security, privacy and surveillance policy, it is instructive to consult Bodea et al. (2013). In the EU privacy regulative framework overview, they emphasize that national regulations of the EU countries have to conform to the European Commission (EC) directives. EU accession sets common standards, and envisaged

[1] Bodea et al. (2013) note that, unlike the EU, the US does not recognize a general right to privacy, nor does a US data protection authority exist; instead, privacy protection is regulated by sectorial regulations (e.g., in healthcare, communications, children's privacy).

convergence of behavior, concerns and attitudes is highly likely. The analysis of the regulation conformity issue goes beyond the scope of this research; however, it is important to note that national legislation and by-laws are not unified across member states.

The evolving standards and the protection of privacy are linked to trust in institutions and trust in the broader European digital agenda and information society, both directly influenced and positively correlated by the EU accession process. In developed countries, trust is important for the emergence and successful development of ICTs and trust in new technologies will increase their adoption and use (Bodea et al., 2013). European citizens should exercise their rights against challenges to privacy that include technological change. There is a discussion of a wide range of privacy protecting measures, often centered on increasing individual control of personal data. This suggests that technological developments have precipitated a re-evaluation of privacy regulation. Findings of the EC-funded research project PRISMS as described by Bodea et al. (2013) recommend using privacy impact assessment (PIA) in information processes as risk assessment, and identifying ways that privacy protection can be included in public policy decision-making (e.g., whether to install video surveillance). PIA is a risk management tool helping organizations to preserve their brand reputation and trust of employees or customers when deploying a new technology, product, service or other initiative involving personal data (see more in Wright & de Hert, 2012). Privacy impact assessment is a tool, a process, a methodology to identify, assess, mitigate or avoid privacy risks and, in collaboration with stakeholders, to identify solutions. It is gaining interest as a new instrument in Europe, although it has been applied for over two decades in the US, New Zealand and other countries outside Europe (Clarke, 2009). Here we do not advocate applying PIA or not, but mention it to raise awareness of privacy gaining importance even in terms of companies' operational costs. Taking privacy into consideration is rapidly penetrating into all aspects of our lives, and this supports the need for research on the issues presented here.

4 Methodology and Data

The qualitative research prior to the construction of the survey questionnaire and pilot testing of the survey tool was conducted in Croatia in 2011 (Budak, Anić & Rajh, 2013). Identical questionnaires translated into national languages were employed in Bosnia and Herzegovina,

Serbia and FYR of Macedonia in 2012. The interviews were conducted in each country by telephone and operated by professional market research agencies under the authors' supervision. The public opinion survey was conducted on a large net sample of 2,006 citizens in total (around 500 citizens per country). In all observed countries the survey was conducted among the adult population aged 18 to 70, on a nationally representative sample regarding regional distribution. Demographic variables about the respondents included questions about gender, age, household size, education and country of residence. The sample statistics are presented in Table 1.

Table 1 Summary Statistics of Sampled Respondents, n=2,006

	%		%
Gender		Country	
Male	49.7	Bosnia and Herzegovina	24.9
Female	50.3	Croatia	25.2
Age		FYR of Macedonia	24.9
18-34	31.5	Serbia	24.9
35-54	37.4	Internet usage	
55-70	31.1	Yes	64.2
Education		No	35.8
Primary school	14.2		
Secondary school	59.9		
University and higher education	25.9		
No answer	0.1		

The 62-item questionnaire included 59 questions in the form of a statement and each item was measured by Likert-scaled items ranging from 1 (strongly disagree) to 5 (strongly agree) and three yes/no questions.[2]

For the purpose of this research we selected three items from the questionnaire, related to the individual level of online privacy concern. These were the following statements:

- Information I send over the internet (e-mail, Facebook and other) could be misused.
- The usage of computers and ICT increases the possibility of personal data manipulation.
- I am concerned about the volume of personal information and data stored on computers that might be misused.

[2] The questionnaire is available from the authors upon request.

The statements were evaluated on a 5-point Likert scale which enabled us to calculate the mean value. On the individual level, the composite measure of online privacy concern was calculated as the unweighted average of responses on the three selected items, in order to obtain the PRICON index. A higher value of the PRICON index denotes more online privacy concern and vice versa (Table 2).

Table 2 Online Privacy Concern PRICON Index, per Country

Country	Online privacy concern
	PRICON index
Croatia	4.26
FYR of Macedonia	4.10
Serbia	3.91
Bosnia and Herzegovina	3.57

Source: Authors' calculations.

Differences in online privacy concern between various groups were compared with analysis of variance (ANOVA) and t-test analysis.

5 Results and Discussion

The ANOVA results indicate that there are statistically significant differences in online privacy concern according to respondents' education, age and country of origin (Table 3). Groups with higher education levels also exhibit higher levels of online privacy concern. The oldest group of respondents exhibits lower levels of online privacy concern when compared with the youngest and middle age groups. Respondents from Croatia exhibit the highest levels of online privacy concern, followed by respondents from FYR of Macedonia and Serbia. Respondents from Bosnia and Herzegovina have the lowest levels of online privacy concern.

Table 3 ANOVA Results – Dependent Variable: Online Privacy Concern

Independent variable	PRICON mean value	St. dev.	N	ANOVA
Education				F=81.40
Primary school or less	3.43	0.83	285	p=0.00
Secondary school	4.01	0.76	1201	
University and higher education	4.12	0.79	519	
Age				F=11.85
18-34	4.00	0.77	632	p=0.00
35-54	4.03	0.79	751	
55-70	3.83	0.85	623	
Country				F=76.89
Croatia	4.26	0.69	506	p=0.00
Serbia	3.91	0.81	500	
Bosnia and Herzegovina	3.57	0.86	500	
FYR of Macedonia	4.10	0.69	500	

T-tests were conducted to test differences in online privacy concern by gender and internet usage (Table 4). The results indicate that there are no statistically significant differences in online privacy concern between males and females. At the same time, there are statistically significant differences in online privacy concern by internet usage groups. Those respondents that use the internet exhibit higher levels of online privacy concern when compared to respondents that do not use the internet. At first, this might sound like a tautology, but items taken into account for the PRICON index also encompass statements for respondents who are concerned about what happens with their personal data provided through other channels in an online setting, although they do not use the internet themselves.

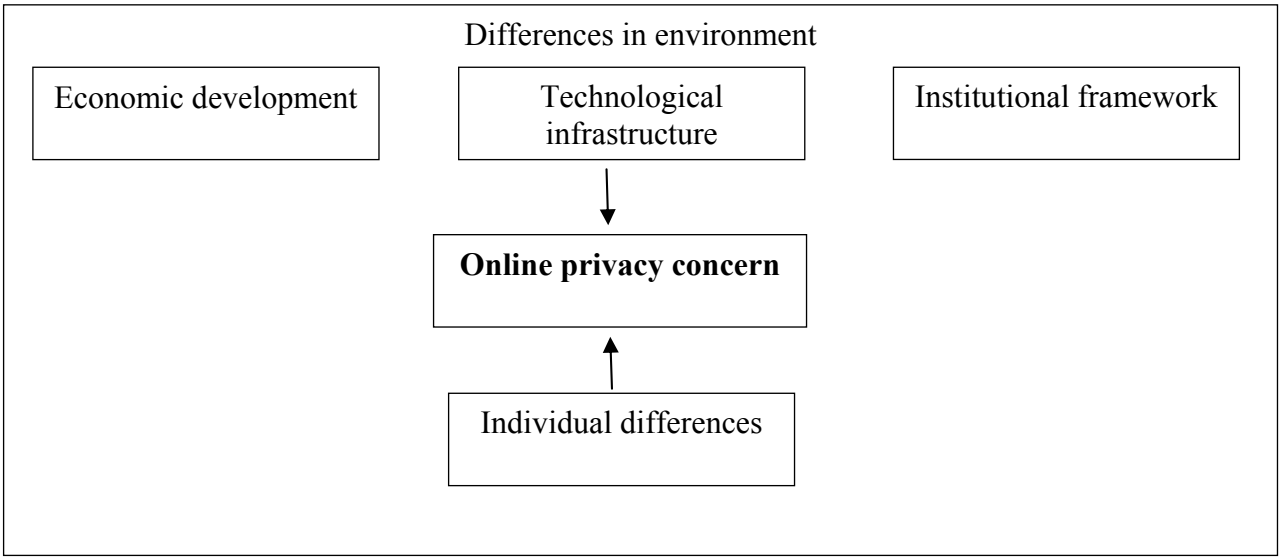
Table 4 T-test Results – Dependent Variable: Online Privacy Concern

Independent variable	PRICON mean value	St. dev.	N	T-test
Gender				t=0.17
Male	3.95	0.77	996	p=0.86
Female	3.96	0.84	1010	
Internet usage				t=9.94
Yes	4.09	0.77	1287	p=0.00
No	3.72	0.82	719	

The analysis shows different socio-demographic attributes of individual respondents to stand as determinants of online privacy concern. On the other hand, people's actual behavior and actions online occur in given circumstances, i.e., in different environments. The environment is marked by economic development, available technological infrastructure and institutional

framework. Online privacy concern thus might be explained by three pillars of a country's development: economic, technological and institutional development (Figure 1).

Figure 1 Contextualizing Online Privacy Concern and Development



The standard indicator of *economic* development is GDP per capita, depicting the country's level of economic development. The *technological* development pillar stands for the country's technological infrastructure in terms of readiness to adopt new technologies and internet penetration. Generally, it could be said that the higher the internet penetration, the higher the online privacy concern. This pillar describes the availability of internet services and new technologies enabling online activities whose usage might raise privacy concerns. The *institutional* set-up is strongly defined by the EU accession process and indicators of democratic rights and liberties. Among the analyzed countries, Croatia is the only EU member state, while the other observed countries are in the process of joining the EU, yet with different status. Serbia and FYR of Macedonia are candidates for joining the EU, while Bosnia and Herzegovina is a potential candidate for accession. These countries are not fully implementing EU legislation, and a major weakness is monitoring and enforcing privacy legislation in practice. Therefore, one could assume that people in the non-EU member states might be less aware of potential privacy risks and less concerned about their privacy. More freedom in the society brings higher awareness of privacy infringements and rising requirements to adequately protect personal information. Table 5 presents selected economic, technological and institutional indicators, and country ranking per level of online privacy concern in descending order. The data are intentionally used for the year 2012, i.e., at the time

of the survey, except for the current EU status. This overview at first glance suggests there is a link between online privacy concern and development: online privacy concern is the highest in Croatia, which in our set of post-transition Western Balkan countries stands as the most developed economy, with advanced infrastructure for online activities, and the only EU member state in the region. However, the pecking order of the other three countries is not that clear-cut. FYR of Macedonia is second with regards to the level of online privacy concern, but in terms of GDP per capita and institutional set-up, it fares somewhat worse than Serbia in third place. The reason for the high level of online privacy concern in FYR of Macedonia is probably the relatively well-developed technological infrastructure – the best among the three non-EU member states. In contrast, Serbia fares well in the institutional set-up, but is lagging behind significantly in the technological pillar. Even Bosnia and Herzegovina, the least developed country in the sample, has larger penetration of new technologies than Serbia. Consequently, it is fair to conclude that all three countries have to put in significant effort to close the gap even to Croatia, let alone other, more developed EU member states. All three countries need to find the recipe to kick-start their economies in terms of GDP per capita growth. Additionally, FYR of Macedonia should focus on improving the institutional set-up and Serbia on advancements on the technological front.

Table 5 Online Privacy Concern, Economic, Technological and Institutional Indicators per Country

Country	Online privacy concern	Economic development	Technological level achieved			Institutional set-up		
	PRICON index	GDP p.c.[1]	Availability of latest technologies[2]	Internet users[3]	Broadband internet[4]	EU status	Political rights[5]	Civil liberties[5]
Croatia	**4.26**	**20,182**	**5.4**	**60.3**	**18.3**	**Member state**	**1**	**2**
FYR of Macedonia	4.10	11,268	4.6	51.9	12.5	Candidate country	4	*3*
Serbia	3.91	12,504	*4.0*	*40.9*	*8.5*	Candidate country	*2*	**2**
Bosnia and Herzegovina	*3.57*	*9,149*	4.4	52.0	10.4	*Potential candidate*	4	*3*

[1] Gross domestic product per capita, PPP, constant international US$ 2011 (source: World Development Indicators, http://www.worldbank.org).
[2] Source: *The Global Competitiveness Report 2011-2012*, World Economic Forum (http://www3.weforum.org/docs/WEF_GCR_Report_2011-12.pdf).
[3] Percentage of individuals using the internet (source: *The Global Competitiveness Report 2011-2012*, World Economic Forum, http://www3.weforum.org/docs/WEF_GCR_Report_2011-12.pdf).
[4] Number of fixed broadband internet subscriptions per 100 population (source: *The Global Competitiveness Report 2011-2012*, World Economic Forum, http://www3.weforum.org/docs/WEF_GCR_Report_2011-12.pdf).
[5] Each country is assigned numerical ratings, with 1 representing the most free and 7 the least free (source: Freedom House, 2015, https://freedomhouse.org/report-types/freedom-world#.VVnTmfAYOI8).

6 Conclusions

In this paper we tried to contextualize online privacy concern with economic development. Previous research and common sense suggest that more developed countries have a higher level of online privacy concern. Indeed, country of origin proved to be a significant antecedent of online privacy concern, measured by the PRICON index. Furthermore, the level of online privacy concern rises with the level of education which is also expected. Less educated people are far less aware of privacy risks connected to internet usage and consequently far less concerned. The relationship between age and online privacy concern could best be described as a reversed U-shaped curve. This is also in line with intuition. Teenagers do not bother too much with the fact that everything they do online stays there permanently. As they age they become more and more aware of potential privacy infringements and risks, especially when starting to use more risky services, such as e-banking. Older people generally use the internet less and are therefore expectedly less concerned about their privacy online.

Croatia, as the relatively most developed country from the sample measured by GDP per capita, has the highest level of online privacy concern. Serbia and Bosnia and Herzegovina also have levels of online privacy concern in line with their levels of development achieved. However, FYR of Macedonia has a high level of online privacy concern considering its level of development. This discrepancy is best explained by the differences in technological advancements.

Obviously, EU accession path and membership play an important role in the development of Western Balkan economies. As countries are implementing reforms necessary to join the EU, people will probably become more aware of privacy issues. On the other hand, businesses and governments will need to follow these advancements by offering a broader scope of more technologically advanced services with better privacy protection. In this sense, the development of a digital society could influence the economic development in terms of GDP per capita. For example, high quality e-government services could reduce bureaucracy and help develop entrepreneurship and SMEs.

One possible policy implication of these conclusions could be better informing the general public about the possibilities and potential of new technologies. Furthermore, it is important

to develop a sound institutional framework and build trust between government, citizens and businesses in order to advance on all fronts. To confirm these conclusions and obtain more tangible results than those presented in this paper, it would be useful to empirically test the concept suggested. Furthermore, a larger pool of post-transition countries is needed to validate the results presented here.

References:

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce*, 21-29.

Acquisti, A., & Grossklags, J. (2007). What Can Behavioral Economics Teach Us About Privacy? *Digital Privacy: Theory, Technologies and Practices*, 363-377.

Anić, I.-D., Rajh, E., & Budak, J. (2014). New information economy in post-transition countries: An economic approach to privacy concern. *Manuscript submitted for publication*.

Belanger, F., Hiller, J., & Smith, W. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*(3-4), 245-270.

Bodea, G., Huijboom, N., van Oort, S., Merel, O., van Schoonhoven, B., Bakker, T., et al. (2013). Security and privacy policy in 21st Century Europe: An overview of privacy and security policy documents in the EU, six Member States and the USA. *PRISMS Collaborative project*.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157-165.

Budak, J., Rajh, E., & Anić, I.-D. (2015). Privacy Concern in Western Balkan Countries: Developing a Typology of Citizens. *Journal of Balkan and Near Eastern Studies, 17*(1), 29-48.

Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer Law & Security Review, 25*(2), 123-135.

Dinev, T., Masssimo, B., Hart, P., Christian, C., Vincenzo, R., & Ilaria, S. (2005). Internet Users, Privacy Concerns and Attitudes towards Government Surveillance-An Exploratory Study of Cross-Cultural Differences between Italy and the United States. *BLED 2005 Proceedings*, *30.*

European Commission. (2011). Attitudes on Data Protection and Electronic Identity in the European Union. *Special Eurobarometer 359*.

European Commission. (2015). Retrieved March 20, 2015, from http://ec.europa.eu/enlargement/countries/check-current-status/index_en.htm

European Court of Human Rights, . (2015). Retrieved March 24, 2015, from http://www.echr.coe.int/Documents/Convention_ENG.pdf

Flaherty, D. H. (1989). *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States.* UNC Press Books.

Fuchs, C. (2011). The Political Economy of Privacy on Facebook. *The internet & Surveillance - Research Paper Series*(9).

Goold, B. J. (2010). How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy. *OVERVÅKNING I EN RETTSSTAT - SURVEILLANCE IN A CONSTITUTIONAL GOVERNMENT*.

Gurung, A., & Jain, A. (2009). Antecedents of Online Privacy Protection Behavior: Towards an Integrative Model. In K. Chen, & A. Fadlalla, *Online Consumer Protection: Theories of Human Relativism* (pp. 151-190). New York: IGI Global.

Haggerty, K., & Gazso, A. (2005). The public politics of opinion research on surveillance and privacy. *Surveillance & Society, 3*(2/3), 173-180.

International Monetary Fund. (2015). The western Balkans : 15 years of economic transition. *Regional Economic Issues Special Report*.

Liu, C., Marchewka, J., Lu, J., & Yu, C. (2004). Beyond concern: A privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(1), 127-142.

Maslow, A. H. (1943). *Psychological review, 50*(4), 370-396.

McKnight, D., & Chervany, N. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce, 15*(4), 35-59.

O'Mahony, C., & Flaherty, P. (2009). The Legal Framework for Data and Consumer Protection in Europe. In C. Kuanchin, & A. Fadlalla, *Online Consumer Protection: Theories of Human Relativism* (pp. 326-346). New York: IGI Global.

Raab, C., & Goold, B. (2011). Protecting information privacy. *Equality and Human Rights Commission Research Report 69*.

Reed, T. (2014). *Digitized Lives: Culture, Power and Social Change in the Internet Era.* New York and London: Taylor & Francis; Routledge.

Regan, P. (1995). *Legislating privacy: Technology, Social values and Public Policy.* Chapel Hill: Blackwell Publishing.

Sheng, H., Nah, F. F.-H., & Siau, K. (2008). An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns. *Journal of the Association for Information Systems: Special Issue, 9*(6), 344-376.

Solove, D. J. (2008a). *Understanding Privacy.* Harvard University Press.

Solove, D. J. (2008b). The New Vulnerability: Data Security and Personal Information. (Radin, & Chander, Eds.) *SECURING PRIVACY IN THE INTERNET*.

Ur, B., & Wang, Y. (2013). A cross-cultural framework for protecting user privacy in online social media. *Proceedings of the 22nd international conference on World Wide Web companion* (pp. 755-762). International World Wide Web Conferences Steering Committee.

Wang, Y., Norcie, G., & Cranor, L. F. (2011). Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social network Sites. *Trust and trustworthy computing*, 146-153.

Warren, S. D., & D, B. L. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.

Westin, A. F. (1970). *Privacy and Freedom* (2nd ed.). New York: Atheneum.

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.

Wright, D., & de Hert, P. (2012). *Privacy Impact Assessment.* Springer Science & Business Media.

ISSN 1846-4238