Routledge
Taylor & Francis Group

Economic Research-Ekonomska Istraživanja

ISSN: 1331-677X (Print) 1848-9664 (Online) Journal homepage: https://www.tandfonline.com/loi/rero20

Perceived quality of privacy protection regulations and online privacy concern

Bruno Škrinjarić, Jelena Budak & Edo Rajh

To cite this article: Bruno Škrinjarić, Jelena Budak & Edo Rajh (2019) Perceived quality of privacy protection regulations and online privacy concern, Economic Research-Ekonomska Istraživanja, 32:1, 982-1000, DOI: 10.1080/1331677X.2019.1585272

To link to this article: https://doi.org/10.1080/1331677X.2019.1585272

Published online: 06 May 2019.

ECONOMIC RESEARCH-EKONOMSKA ISTRAŽIVANJA
2019, VOL. 32, NO. 1, 982–1000
https://doi.org/10.1080/1331677X.2019.1585272

Perceived quality of privacy protection regulations and online privacy concern

Bruno Škrinjarić, Jelena Budak and Edo Rajh

The Institute of Economics, Zagreb, Croatia

ABSTRACT

This study examines the impact of regulation as an antecedent of online privacy concern. Previous research found that perceived effectiveness and enforcement of regulatory policies reduce online privacy concern; however, it does not explain what factors influence this relationship. Based on the survey data, the empirical analysis is conducted on a large sample of internet users in Croatia. Our methodology consists of two parts: first, we use confirmatory factor analysis to validate the latent constructs used in the main model; and then we proceed with model estimation using OLS and ordered probit techniques. This study fills the gap in the existing body of knowledge by analysing different perceptions of the existing legislation and government effort to protect online privacy in the context of sociodemographic characteristics of respondents, computer anxiety, individual desire to maintain control of personal information online, as well as intensity and diversity of online activities. Our results indicate that perceived effectiveness of government regulation reduces online privacy concern whereas computer anxiety has a major positive impact on online privacy concern. These findings might be useful for national policy-makers and for business strategies, especially in the context of the GDPR regulation introduced in 2018.

ARTICLE HISTORY
Received 5 June 2018
Accepted 12 December 2018

KEYWORDS
Regulation; data protection; online privacy concern; Croatia

JEL CLASSIFICATIONS
D1; K2; D9

1. Introduction

Government regulation affects all domains of everyday life. Both formal institutions, in terms of laws, regulations and rules, and informal institutions, such as culture, tradition or inherited social norms, affect economic activity (North, 1990) and shape the behaviour of consumers and businesses. The role of regulators has changed in the digital era (Henderson, 2015), where enforcement of privacy legislation has become a major issue (Reay et al., 2011). Living in the digitalised world has increased concern about online privacy (Malhotra et al., 2004; Dinev & Hart, 2006; Ginosar & Ariel, 2017). These two simultaneous processes raise questions on if and how government regulations impact the level of privacy concern in the online environment.

CONTACT Bruno Škrinjarić bskrinjaric@eizg.hr

Past research has examined the impacts of regulation, legal and regulatory policies on online privacy concern (Lwin, Wirtz & Williams, 2007), indicating that internet users often have limited knowledge and resources to protect their data and thus they might rely on institutional laws and regulations. Rust, Kannan & Peng (2002) show that regulation is considered to be important in protecting online privacy, while the study of Lwin, Wirtz & Williams (2007) demonstrates that perceived effectiveness of regulatory policies and their enforcement reduces consumer online privacy concern. The literature recognises there are different concepts of information privacy all characterised by the large complexity of the model (see e.g., Dinev et al., 2013; Smith et al., 2011; Xu et al., 2011; Li, 2012).

The findings, however, do not explain what factors lie behind the perceived effectiveness of government regulations in terms of demographic characteristics, diversity of online activities, computer anxiety and individual desire to take control over personal data when online. This research fills the gap and provides insight into a large sample of internet users in the post-transition country of Croatia. The aim of the research is to contribute to the scholarly debate on whether the perceived quality and effectiveness of the regulatory framework determine online privacy concern of internet users, i.e., consumers and/or citizens. This study is supported by the procedural fairness theory, as systemised by Li (2012). Procedural fairness approach argues that privacy concern might be alleviated by employing fair privacy protecting practices and procedures, including government regulations and business policies. Perceptions of regulations effectiveness might significantly differ from the actual quality of regulation; however, what citizens think about regulations is shaping their subjective opinion about privacy and behaviour related to the level of privacy concern. People who are more or less concerned about the risk of privacy intrusion, or any kind of privacy breaches would shape their online behaviour accordingly by employing protective strategies, hiding information, providing false information or even sustaining of internet usage for certain activities (Wirtz et al., 2007). If so, what business opportunities in improving relations with clients arise, in particular in the context of the upcoming GDPR? Policy-makers and regulators will get feedback on the impact of regulatory control as perceived by internet users in Croatia and might improve the regulatory framework or public communication strategies accordingly.

The paper is structured as follows. First, we provide a brief description of the regulatory framework regarding privacy and personal data protection and a literature review in this field. Next, we explain the variables in our model and methodology applied, followed by the section on the survey data. The results of regression analyses are presented and discussed in sections five and six. Policy implications are offered in the last section, together with concluding remarks and suggested lines of future research.

2. Regulative framework regarding privacy

In order to understand the relationship between regulation and online privacy concern, one needs to get an overview on how privacy and personal data are dealt with in the legislative and regulatory framework.

Privacy regulation and legislation have a rather long tradition, since the first rules on integrity of home and business premises were introduced in Britain in the eighteenth century (Henderson, 2015). The privacy protection regulation has evolved somewhat differently in the United States when compared to Europe (and other parts of the world). The development of automatic data processing and data transmission worldwide and across national borders raised the issue of privacy protection in relation to personal data. From 1980 onwards, privacy protection laws have been introduced in many countries to prevent unlawful storage of personal data, abuse or unauthorised disclosure of data and similar privacy breaches. At the same time, the most developed countries in the world recognised that such restrictions implemented in national legislations could be too restrictive for the free flow of information and digital transfer of data required for further development of financial services, the ICT sector and trade. Thus, in 1980, the OECD developed guidelines which would help to harmonise national privacy legislation and, while upholding human rights, would at the same time prevent interruptions in international flows of data (OECD, 1980).

In the European regulation, the form and scope of the right to data protection vary considerably in national jurisdictions (Koops et al., 2017). In some EU countries, privacy is a constitutional category, but objects of protection in constitutional rights to privacy vary, and personal data is one of them. In light of this research, recent developments in the regulatory framework for the EU and Croatia, and other countries trading and exchanging data with EU members in terms of introducing the General Data Protection Regulation (GDPR) in 2018 might be very important (more on EU and Croatian regulation is provided in Appendix 1).

In the business environment, profit-making business models rely upon collecting personal information and profiling clients who pay for online services by disclosing personal information (Rauhofer, 2013). However, people tend to maintain control of their personal data and this might be the complementary variable determining their level of online privacy concern. On the one hand, internet users might call for more effective government regulations to protect them, and on the other, individuals employ other risk-mitigating actions. Individuals who feel fearful about computers, being afraid of losing their data for example (Parasuraman & Igbaria, 1990; Thatcher & Perrewe, 2002; Korzaan & Boswell, 2008), behave less comfortably when working with computers and show higher privacy concern (Stewart & Segars, 2002).

As previously stated, the quality of regulation is expected to reduce concerns about privacy intrusions (Lwin, Wirtz & Williams, 2007; Rust, Kannan & Peng, 2002). The role of data protection agencies as national regulators in the EU is crucial; however, their capacities to comprehend new technologies are questionable and this could pose a huge problem given the GDPR requirements (Raab & Szekely, 2017). Comparative survey study on privacy showed that 'citizens (especially in Hungary) do not consider themselves knowledgeable about laws protecting information in government departments', and only a small share of knowledgeable people consider legislation effective (The Surveillance Project, 2008:10). In the online context, the situation looks equally puzzling. More recent studies also recognise state privacy policies and regulations as an important domain for online privacy research (Ginosar & Ariel, 2017), in particular having in mind that internet users have limited knowledge and resources to assess

data security and they rely on laws to protect them (Acquisti et al., 2015; Dommeyer & Gross, 2003). Opposed to this view, advocates of the self-regulation principle suggest that companies and e-business have strong incentives to introduce privacy protection rules to keep their online clients satisfied (Ginosar & Ariel, 2017).

This kind of empirical evidence is lacking for Croatia and the region. Peštek et al. (2011) showed that consumers in Bosnia and Herzegovina consider company privacy policy an important factor for participating in e-transactions. They suggest that e-merchants should develop an online trust model that among other factors would include privacy protection. However, there is a scarcity of empirical research on perceptions as to how state regulations protect consumers' personal data and how they affect internet users' privacy concerns.

3. Conceptual model and methodology

The conceptual model we empirically test is presented in Figure 1. It indicates the direction of relationship of each independent variable to online privacy concern (or possibly a significant impact in either direction, as there have been contrasting findings in the existing literature).

The dependent variable in the model is online privacy concern (*opc*). The intensity or range of such concern is subjective and difficult to measure, so we have taken the measurement scales for privacy concern developed in the literature and adapted them for the internet environment. One of the first scales of concern for information privacy (CFIP) was developed by Smith, Milberg & Burke (1996) to measure collection, errors, secondary use and unauthorised access to information as dimensions of an individual's concern for privacy. Our *opc* scales are based on Malhotra, Kim & Agarwal's (2004) construct of internet users' information privacy concerns (IUIPC). This better reflects concerns in the online environment because it comprises attitudes towards the collection of personal information, control over personal information and awareness of privacy practices of companies gathering personal information (Anić et al., 2018).

The determinants of online privacy concern have been taken from the existing literature on antecedents of this concern and adapted them for the online environment.[1]

The perceived degree of regulatory control (*reg*) and its efficacy is measured by three items. Respondents were asked to declare if the existing country legislation and government direction are sufficient to protect online privacy (Lwin, Wirtz &

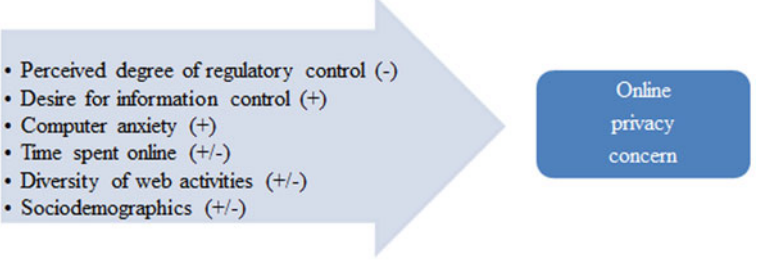

Figure 1. Conceptual model.

Williams, 2007) or whether more strict regulation should be put in place to protect personal privacy online (Wirtz, Lwin & Williams, 2007).

Based on past studies (Yeh et al., 2018; Hajli & Lin, 2016; Malhotra, Kim & Agarwal, 2004; Smith, Milberg & Burke, 1996), we include desire for information control (*ctrl*) into the model. It is measured with four items related to the individual's desire or inclination towards the control of the collection, usage, and sharing of their personal data on the internet. Intuitively, fear of computers and technology, a phenomenon known in the literature as computer anxiety (*ca*), might increase the level of online privacy concern (Stewart & Segars, 2002).

The intensity of internet usage in terms of time spent online *(time)* and the type of online service or activity performed *(web)* could significantly determine the level of online privacy concern. Heavy users and advanced users of the internet might be more aware of privacy risks when online and therefore more concerned. However, it might be the opposite, if these internet users are so internet-addicted that they just do not feel any concern for their online privacy.

The privacy concern of internet users might be more or less evident depending on the socio-demographic characteristics of individual respondents (e.g., Zhang et al., 2002; Hoy & Milne, 2010; Zukowski & Brown, 2007; Zhang et al., 2013). First, we included basic demographic characteristics of the internet users into the model: gender *(gender)*, age *(age)*, level of education attained *(educ)*, occupation (*ocu*), size of the household *(hh)* and monthly household income (*income*). Here, past research has reached no consensus on the significance and direction of relationships, so it would be interesting to shed more light on the individual socio-demographics and online privacy concern nexus. Further, we wanted to examine if there were any regional differences across the five regions in Croatia (*region)* and among respondents living in larger or smaller places of residence *(size)*. The difference in the place of residence size is a proxy for capturing differences between the urban and rural environment in Croatia. People living in rural environments might be less concerned about privacy when online, because they openly interact more with each other and privacy is harder to conserve in everyday life in smaller places.

The conceptual model presented in Figure 1 is tested using the following model:

$$OPC_i = \alpha + \beta_1 REG_i + \beta_2 CTRL_i + \beta_3 CA_i + \beta_4 TIME_i + \beta_5 WEB_i + \gamma' X_i + \epsilon_i, \qquad (1)$$

where online privacy concern, *opc*, is a dependent variable, *reg* is perceived degree of government regulatory control, *ctrl* is need for control of personal information online, *ca* is computer anxiety, *time* is number of hours spent online during a day, *web* is diversity of internet activities and X is a matrix of other socio-demographic characteristics of respondents used in the model. All of the latent variables used in the model above (*opc, reg, ctrl* and *ca*) enter the equation in their standardised form, i.e., with a mean of 0 and standard deviation of 1; hence, they are interpreted in terms of standard deviations. Items used to calculate these variables (presented in Table 1) were measured on a Likert scale ranging from 1 (totally disagree) to 5 (totally agree).

Table 1. Variables in Model 1.

Variable	Description
Online privacy concern (opc)	Index computed from these six items*: • I am concerned about my online privacy. • All things considered, the internet could 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. (Cronbach alpha 0.86, inter-item correlation 0.79)
Degree of regulatory control (reg)	Index computed from these three items*: • The existing laws in my country are sufficient to protect people's online privacy. • The government is doing enough to ensure that citizens are protected against online privacy violations. • There should be tougher regulations by the government to protect personal privacy online. (Cronbach alpha 0.68, inter-item correlation 0.40)
Individual's desire for information control (ctrl)	Index computed from these four items*: • My online privacy is really a matter of my right to exercise control and autonomy over decisions about how my information is collected, used, and shared. • My control of personal information lies at the heart of my privacy. • Personal information should not be used for any purpose unless it has been authorised by that person. • When people give personal information for some reason, it should never be used for any other reason. (Cronbach alpha 0.81, inter-item correlation 0.27)
Computer anxiety (ca)	Index computed from these three items*: • Computers are a real threat to privacy in this country. • I am anxious and concerned about the pace of automation in the world. • I am easily frustrated by increased computerisation in my life. (Cronbach alpha 0.72, inter-item correlation 0.82)
Time (time)	Number of hours in a typical day the respondent spends on the internet
Diversity of online activities (web)	Number of different activities the respondent uses the internet for. In total there were 15 of them: receiving and sending e-mails, using chat/instant message services (e.g., WhatsApp), downloading music and/or movies, playing online games, paying bills/e-banking, attending online courses, online shopping, live video or audio streaming, watching videos over the internet (e.g., YouTube), making phone calls over the internet (e.g., Skype), using social networks (e.g., Facebook, Twitter, Instagram), following daily news, looking for general information (e.g., Google, Wikipedia), using online forums, using public services available online (e.g., tender applications, online forms, filing taxes online, etc.)
Gender (gender)	1 = male, 0 = female
Age (age)	Age of respondent
Education (educ)	Highest achieved level of education: 1 = primary school or less; 2 = secondary education; 3 = tertiary education/college, university; 4 = master's degree/doctoral title
Occupation (ocu)	Occupation of respondent: 1 = owner of the company/craft (own-account worker); 2 = manager/official; 3 = professional (highly educated, e.g., medical doctor, lawyer, bookkeeper, etc.); 4 = technician/clerk; 5 = worker; 6 = retired; 7 = student; 8 = unemployed
Household (hh)	Number of people living in respondent's household
Income (income)	Total monthly income of respondent's household (in HRK**): 1 = 2,500 or less; 2 = 2,501–5,000; 3 = 5,001–7,500; 4 = 7,501–10,000; 5 = 10,001–12,500; 6 = 12,501–15,000; 7 = more than 7,500
Region (region)	Five Croatian regions*** (based on 21 Croatian counties): 1 = Zagreb; 2 = Western Croatia; 3 = Eastern Croatia; 4 = Central Croatia; 5 = Southern Croatia
Size of place of residence (size)	Number of inhabitants in respondent's place of residence: 1 = 10,000 or less; 2 = 10,001–50,000; 3 = 50,001–100,000; 4 = more than 100,000

Notes:
*The items were measured on a 5-point Likert scale ranging from 1 (totally disagree) to 5 (totally agree). All indexes were calculated as a simple average of their items.
**1 EUR = 7.529 HRK (2016 average).
***Defined in Table A1 in the Appendix 2.

4. Data description

We use survey data collected from November 2015 to March 2016 on a sample of internet users in Croatia. The survey was conducted by a computer-assisted telephone interviewing (CATI) method. An online phone book was used as a sampling frame and secondary data (Stilus Media) were used to assess the number of internet users in Croatia. The sample was created based on a one-way stratification by 21 counties, where the sample allocated to each stratum was proportional to the assessed number of internet users in each stratum. Within each stratum a

Table 2. Descriptive Statistics.

Variable	n	Mean	St. Dev.	Min.	Max.
Online privacy concern	2,060	3.56	0.96	1	5
Degree of regulatory control	2,060	3.06	0.6	1	5
Control of personal information online	2,060	4.56	0.57	1	5
Computer anxiety	2,060	2.94	1.06	1	5
Time spent online	2,060	3.22	2.87	0.5	24
Diversity of online activities	2,060	9.05	2.68	1	15
Gender					
Male	1,030	0.5	0.5	0	1
Female	1,030	0.5	0.5	0	1
Age	2,060	39.83	12.91	18	84
Education*					
Primary or less	17	0.01	0.09	0	1
Secondary	1,035	0.5	0.5	0	1
Tertiary	945	0.46	0.5	0	1
PhD or post-grad	63	0.03	0.17	0	1
Occupation*					
Self-employed	42	0.02	0.14	0	1
Manager	44	0.02	0.14	0	1
Professional	616	0.3	0.46	0	1
Technician/clerk	373	0.18	0.39	0	1
Worker	508	0.25	0.43	0	1
Retired	180	0.09	0.28	0	1
Student	180	0.09	0.28	0	1
Unemployed	103	0.05	0.22	0	1
Other	14	0.01	0.08	0	1
Number of people in household	2,060	3.52	1.26	1	12
Household income*					
2,500 or less	51	0.02	0.16	0	1
2,501–5,000	305	0.15	0.36	0	1
5,001–7,500	451	0.22	0.41	0	1
7,501–10,000	601	0.29	0.45	0	1
10,001–12,500	274	0.13	0.34	0	1
12,501–15,000	197	0.1	0.29	0	1
More than 7,500	181	0.09	0.28	0	1
Region*					
Zagreb	544	0.26	0.44	0	1
Western Croatia	262	0.13	0.33	0	1
Eastern Croatia	387	0.19	0.39	0	1
Central Croatia	461	0.22	0.42	0	1
Southern Croatia	406	0.2	0.4	0	1
Size of place of residence*					
10,000 or less	279	0.14	0.34	0	1
10,001–50,000	731	0.35	0.48	0	1
50,001–100,000	311	0.15	0.36	0	1
More than 100,000	739	0.36	0.48	0	1

Note:
*These variables were transformed into dummy variables for each possible outcome, so the means in this case actually represent the percentage of respondents with a given outcome for every variable.

combination of random and systematic sampling was applied. Pages from the phone book were selected using simple random sampling procedure. Sample units within each page were selected applying a systematic sampling procedure. Altogether, more than 19,000 calls to participate in the survey were made. With a response rate of 10.8%, the final sample consisted of 2060 internet users aged 18 years or older. The sample size was determined with the goal of decreasing the margin of error, especially for subsample comparisons. The descriptive statistics of variables in Model 1 are presented in Table 2.

5. Results

Prior to estimation, latent constructs in Model 1 were validated using confirmatory factor analysis. Figure 2 presents standardised estimates, and root mean square error of approximation of 0.062 confirms the usage of the aforementioned items to measure the latent constructs.

The correlation matrix of all variables in Model 1, other than socio-demographic characteristics of respondents, shows all the regressors are very weakly correlated among themselves, indicating a low risk of multicollinearity problems (Table 3).

Model 1 was estimated using the OLS method in Stata 15 software. The model was estimated three times by subsequently adding more covariates – version 1 is a simple case where *opc* is regressed on other latent variables in the model; version 2 further includes two indicators on internet usage; version 3 includes all the personal characteristics of the respondents (Table 4).

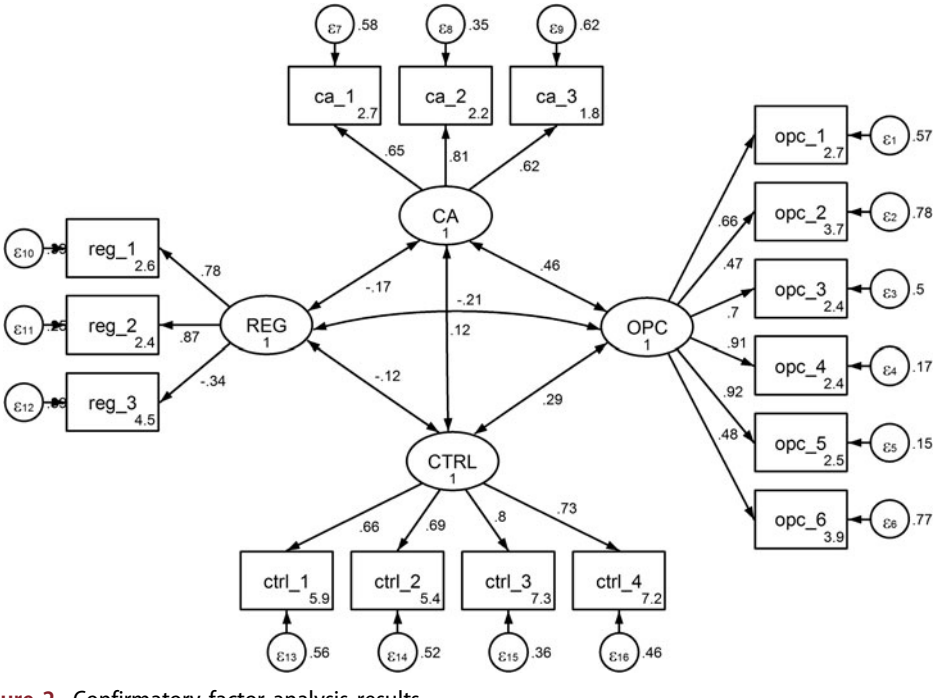

Figure 2. Confirmatory factor analysis results.

Table 3. Correlation matrix of variables in Model 1.

Variable	OPC	REG	CA	CTRL	TIME	WEB
OPC	1					
REG	−0.0436	1				
CA	0.4614	−0.0554	1			
CTRL	0.3376	0.1053	0.1059	1		
TIME	−0.0799	−0.0408	−0.152	−0.0865	1	
WEB	−0.1289	−0.0177	−0.1654	−0.0765	0.3871	1

Note: OPC, REG, CA and CTRL variables were analysed in their standardized form.

Table 4. OLS Estimation Results.

	Version 1		Version 2		Version 3	
Degree of regulatory control	−0.051***	(0.019)	−0.051***	(0.019)	−0.049***	(0.019)
Computer anxiety	0.427***	(0.019)	0.423***	(0.019)	0.423***	(0.019)
Control of personal information online	0.298***	(0.019)	0.297***	(0.019)	0.312***	(0.020)
Time spent online			0.009	(0.007)	0.007	(0.007)
Diversity of online activities			−0.018**	(0.008)	−0.022***	(0.008)
Male					0.021	(0.038)
Age					−0.005**	(0.002)
Household					0.011	(0.016)
Education level (primary benchmark)						
Secondary					−0.392*	(0.208)
Tertiary					−0.379*	(0.212)
Post-grad					−0.177	(0.239)
Occupation (self-employed benchmark)						
Manager					−0.204	(0.182)
Professional					−0.253*	(0.139)
Technician/clerk					−0.126	(0.139)
Worker					−0.109	(0.139)
Retired					−0.083	(0.152)
Student					−0.309**	(0.150)
Unemployed					−0.264*	(0.158)
Other					−0.153	(0.260)
Place of residence (10,000 or less benchmark)						
10,001–50,000					0.009	(0.060)
50,001–100,000					−0.022	(0.071)
More than 100,000					0.066	(0.066)
Income (2,500 or less benchmark)						
2,501–5,000					0.006	(0.129)
5,001–7,500					−0.012	(0.127)
7,501–10,000					−0.024	(0.127)
10,001–12,500					−0.009	(0.134)
12,501–15,000					0.045	(0.138)
More than 15,000					0.067	(0.140)
Region (Zagreb region benchmark)						
Western Croatia					0.085	(0.065)
Eastern Croatia					−0.002	(0.062)
Central Croatia					0.026	(0.066)
Southern Croatia					−0.010	(0.059)
Constant	0.000	(0.018)	0.130**	(0.066)	0.837***	(0.307)
N	2,060		2,060		2,060	
Adj. R^2	0.2988		0.3001		0.3023	

Notes: Standard errors in parentheses;
*$p < 0.10$,
**$p < 0.05$,
***$p < 0.01$.
Benchmark levels of certain socio-demographic variables were chosen based on our intuition.

Prior to analysis of the results we would like to point out that, as we are dealing with a cross-section type of dataset (as opposed to panel structure), our analysis only reveals correlations or associations (rather than causations) and all the following results should be interpreted as such.

All three social-psychological factors (perceived degree of regulatory control, computer anxiety and control of personal information online) were shown to be of statistical significance, in all three versions of Model 1 at a one-percent significance level. A unit standard deviation increase in perceived degree of regulatory control is associated with a decrease of 0.049 to 0.051 standard deviations in online privacy concern.

A one-standard deviation increase in computer anxiety is associated with an increase of 0.423 to 0.427 standard deviations in online privacy concern. Similarly, a unit standard deviation increase in an individual's desire for information control when online relates to an increase of between 0.297 and 0.312 standard deviations in online privacy concern. Turning now to version 2 of Model 1, the measured intensity of internet usage in terms of time and range of activities performed online is less important for online privacy concern. Namely, out of two analysed experience factors (time spent online and diversity of online activities), only diversity of online activities showed to be of statistical significance. A unit increase in diversity of online activities translates to a decrease of between 0.018 and 0.022 standard deviations in online privacy concern.

Finally, in the third version of Model 1, out of eight analysed demographic factors, only age, education level and occupation showed to be of statistical significance. Somewhat unexpectedly, older people express less concern, since a one-year increase in a person's age is associated with a decrease of 0.005 standard deviations in online privacy concern. The concern drops with higher level of education attained. Compared to someone who has completed only a primary level of education, secondary and tertiary education qualifications make a person less sensitive to online privacy concern by 0.392 and 0.379 standard deviations, respectively. Any further education degree has no significance for perceived online privacy concern. Certain occupation groups also showed to be statistically significant when explaining variation in online privacy concern levels. Namely, compared to people who are self-employed, professional workers are less concerned for their online privacy by 0.253 standard deviations; students are also less concerned by 0.309 standard deviations and those unemployed by 0.264 standard deviations. Gender, household size, place of residence size, income group or region did not bear any significance in explaining online privacy concern variation. The most consistent result of this analysis is also the one of our key interests in this research – perceived degree of regulatory control. As we added more and more controls in our original version (version 1) of Model 1, the estimated coefficient for this variable proved to be very robust with very little variation, which only adds validity to these results.

Although the analysis using standard deviations as the unit of measure in the dependent variable is mathematically sound, it lacks a practical application in the real world. Most people are not used to thinking in terms of standard deviations, so another approach predicting the probability of each outcome of the online privacy concern might be more intuitive to explain. Bearing this in mind, and also as a robustness check, the full specification (version 3) of Model 1 was estimated using the ordered probit estimation procedure.

In our case, the online privacy concern (*opc*) dependent variable can take five different categories (outcomes) on the Likert scale, ranging from 1 to 5 (1 – 'Not

concerned at all', 2 – 'Unconcerned', 3 – 'Neither concerned nor unconcerned', 4 – 'Concerned', 5 – 'Very concerned'). These discrete outcomes of *opc* were obtained by rounding the value of *opc* to the nearest integer for each respondent. Other latent covariates (*reg*, *ctrl* and *ca*) still enter the equation in their standardised form and are hence interpreted in terms of standard deviations, but the dependent variable *opc* now enters as a discrete variable. Table 5 shows the results of ordered probit estimations.

The ordered probit estimation results generally confirm the OLS findings. An increase of one standard deviation from the mean is associated with a 0.1 to 1.6 percent increase in probability to be unconcerned or neither concerned nor unconcerned for online privacy. For the last two outcomes of the *opc* variable, the signs are negative, meaning that an increase in one standard deviation in the perceived regulatory effectiveness is estimated to raise the probability to be concerned or very concerned for online privacy by one percent and 1.8 percent, respectively. This finding is in line with the previous OLS result confirming that internet users who perceive regulation to be effective are likely to be less concerned about online privacy.

The next result indicates that a unit standard deviation increase from the mean in computer anxiety translates to a decrease in probability of being unconcerned or neither concerned nor unconcerned for online privacy (from 0.6 and 8.1 to 11.3 percent) and to an increase in probability to be concerned or very concerned for online privacy by 7.1 and 12.9 percent, respectively. This result is also consistent with previous OLS results according to which people who have fears and feel anxious working with computers are more concerned about online privacy.

With regard to control of personal information, the results are as expected. A unit standard deviation increase in this variable relates to a 0.4, 6.4 and 8.9 percent increase in probability to be unconcerned or neither concerned nor unconcerned for online privacy. For the last two outcomes, one standard deviation increase in control of personal information increases the probability to be concerned or very concerned for online privacy by 5.6 and 10.1 percent, respectively. The assumption that stronger desire to maintain control leads to higher online privacy concern is confirmed.

Time spent online again was not significant, contrary to the diversity of online activities. The ordered probit estimates show that one unit increase in diversity of online activities is associated with an increase in probability to be neither concerned nor unconcerned for online privacy by 0.5 and 0.7 percent, and a decrease in probability to be concerned or very concerned for online privacy by 0.5 and 0.8 percent, respectively.

Age is shown to be of statistical significance, albeit with a very weak impact. Increase in a person's age by one year correlates to an increase in probability to be not concerned or neither concerned nor unconcerned for online privacy by 0.1 and 0.2 percent, respectively, and at the same time to a decrease in probability to be concerned or very concerned for online privacy by the same percentage (0.1 and 0.2 percent, respectively).

The findings about the respondents' level of education are in line with the findings on occupation. Students and professionals are more educated internet users. Therefore, compared to the self-employed, it is not surprising that students are more

Table 5. Ordered probit estimation results.

	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
Degree of regulatory control	0.001**	0.011***	0.016***	−0.010***	−0.018***
	(0.000)	(0.004)	(0.005)	(0.003)	(0.006)
Computer anxiety	−0.006***	−0.081***	−0.113***	0.071***	0.129***
	(0.001)	(0.006)	(0.008)	(0.007)	(0.007)
Control of personal information online	−0.004***	−0.064***	−0.089***	0.056***	0.101***
	(0.001)	(0.005)	(0.007)	(0.006)	(0.007)
Time spent online	−0.000	−0.001	−0.002	0.001	0.002
	(0.000)	(0.001)	(0.002)	(0.001)	(0.002)
Diversity of online activities	0.000**	0.005***	0.007***	−0.005***	−0.008***
	(0.000)	(0.002)	(0.002)	(0.002)	(0.003)
Male	−0.000	−0.004	−0.005	0.003	0.006
	(0.001)	(0.008)	(0.011)	(0.007)	(0.012)
Age	0.000**	0.001***	0.002***	−0.001***	−0.002***
	(0.000)	(0.000)	(0.001)	(0.000)	(0.001)
Household	0.000	0.000	0.001	−0.000	−0.001
	(0.000)	(0.003)	(0.005)	(0.003)	(0.005)
Education level (primary benchmark)					
Secondary	0.003***	0.068***	0.142**	−0.020	−0.193*
	(0.001)	(0.019)	(0.062)	(0.026)	(0.104)
Tertiary	0.003***	0.062***	0.135**	−0.016	−0.185*
	(0.001)	(0.020)	(0.063)	(0.025)	(0.106)
Post-grad	0.002	0.038	0.095	0.003	−0.137
	(0.001)	(0.026)	(0.071)	(0.026)	(0.114)
Occupation (self-employed benchmark)					
Manager	0.002	0.033	0.058	−0.021	−0.071
	(0.002)	(0.032)	(0.055)	(0.023)	(0.068)
Professional	0.003**	0.048**	0.078*	−0.035***	−0.093*
	(0.001)	(0.021)	(0.043)	(0.011)	(0.056)
Technician/clerk	0.002*	0.034	0.060	−0.022**	−0.073
	(0.001)	(0.021)	(0.043)	(0.010)	(0.056)
Worker	0.001	0.021	0.040	−0.012	−0.051
	(0.001)	(0.021)	(0.043)	(0.009)	(0.057)
Retired	0.001	0.019	0.037	−0.011	−0.046
	(0.001)	(0.023)	(0.047)	(0.012)	(0.061)
Student	0.005**	0.074***	0.106**	−0.060***	−0.125**
	(0.002)	(0.027)	(0.045)	(0.020)	(0.058)
Unemployed	0.004*	0.056**	0.087*	−0.043**	−0.104*
	(0.002)	(0.028)	(0.047)	(0.021)	(0.060)
Other	0.000	0.002	0.005	−0.001	−0.006
	(0.002)	(0.037)	(0.080)	(0.015)	(0.104)
Place of residence (10,000 or less benchmark)					
10,001–50,000	−0.000	−0.002	−0.002	0.001	0.002
	(0.001)	(0.013)	(0.017)	(0.011)	(0.019)
50,001–100,000	0.001	0.013	0.016	−0.012	−0.018
	(0.001)	(0.016)	(0.020)	(0.014)	(0.022)
More than 100,000	−0.001	−0.010	−0.014	0.008	0.016
	(0.001)	(0.013)	(0.019)	(0.012)	(0.021)
Income (2,500 or less benchmark)					
2,501–5,000	−0.000	−0.007	−0.009	0.006	0.010
	(0.002)	(0.028)	(0.036)	(0.025)	(0.041)
5,001–7,500	−0.000	−0.006	−0.008	0.005	0.009
	(0.002)	(0.028)	(0.036)	(0.025)	(0.040)
7,501–10,000	−0.000	−0.001	−0.001	0.001	0.002
	(0.002)	(0.028)	(0.035)	(0.025)	(0.040)
10,001–12,500	0.000	0.003	0.004	−0.003	−0.004
	(0.002)	(0.029)	(0.037)	(0.027)	(0.042)
12,501–15,000	−0.002	−0.024	−0.036	0.020	0.042
	(0.002)	(0.029)	(0.039)	(0.026)	(0.045)
More than 15,000	−0.001	−0.020	−0.028	0.017	0.033
	(0.002)	(0.029)	(0.040)	(0.026)	(0.045)

(*continued*)

Table 5. Continued.

	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
Region (Zagreb region benchmark)					
Western Croatia	−0.001	−0.010	−0.014	0.009	0.016
	(0.001)	(0.013)	(0.019)	(0.011)	(0.022)
Eastern Croatia	0.000	0.003	0.004	−0.003	−0.005
	(0.001)	(0.013)	(0.017)	(0.012)	(0.020)
Central Croatia	−0.001	−0.011	−0.015	0.009	0.017
	(0.001)	(0.013)	(0.019)	(0.011)	(0.022)
Southern Croatia	0.000	0.000	0.001	−0.000	−0.001
	(0.001)	(0.012)	(0.016)	(0.011)	(0.019)
N	2,060	2,060	2,060	2,060	2,060

Notes: Standard errors in parentheses.
*$p < 0.10$,.
**$p < 0.05$,.
***$p < 0.01$.

prone to be not concerned at all (0.5 percent) or unconcerned (7.4 percent), and less likely to be concerned (–6 percent) or very concerned (–12.5 percent). The same stands for professionals who, compared to the self-employed, are more likely not to be concerned at all (0.3 percent) or to be unconcerned (4.8 percent), and unlikely to be concerned (–3.5 percent) or very concerned about online privacy (–9.3 percent). For both students and professionals, the highest probability is observed to be neither unconcerned nor concerned (10.6 for students and 7.8 for professionals). Other variables in the model were not found to be significant.

6. Discussion

Our study indicates that internet users who perceive regulation to be effective are less likely to be concerned about online privacy, which is in line with the past studies (e.g., Lwin, Wirtz & Williams, 2007). The impact magnitude of regulation as an antecedent to online privacy concern is quite stable as more controls were added to the initial estimates (as we move from model version 1 to version 3), suggesting our baseline model to be quite robust.

Insofar as it considers other personal attributes of internet users, basically, 'the older you get, the less concerned you are about your online privacy'. This result is contrary to previous findings that older internet users tend to be more concerned about privacy (Zukowski & Brown, 2007; Zhang, Chen & Lee, 2013). One of the possible explanations is that older people may not be acquainted with online privacy issues, thus the lack of privacy awareness is related to the lower levels of privacy concern (Dommeyer & Gross, 2003). Educational attainment estimates suggest that the probability of being less concerned rises if the respondent belongs to the more educated group of internet users. More educated internet users in our sample tend to be more exposed to the internet in their everyday life (e.g., students or professionals) and perhaps they do not even think about privacy when online.

Computer anxiety has the strongest (positive) associations to online privacy concern. Internet users in Croatia are concerned about their privacy primarily if they experience fear of computers and of technology in general. Our study thus reconfirms the findings of Stewart & Segars (2002), and early findings of Parasuraman & Igbaria

(1990) conducted well before the global digitalisation wave. It is interesting that nowadays internet users should feel any computer anxiety at all, and that this fear proves to be significant for privacy concern online. Concerns are also increased for those users who feel a strong desire to maintain control and somewhat alleviated for users who believe regulations are protecting their privacy. This result, combined with the observed significance of the variable denoting diversity of online activities, leads us to conclude that more skilled internet users feel less concern about online privacy.

7. Conclusion

The findings of this research shed light on the privacy protection regulations and online privacy concern nexus. The study fills a gap in the existing body of knowledge by analysing different perceptions of the existing legislation and government effort to protect online privacy in the context of socio-demographic characteristics of respondents, computer anxiety, individual desire to maintain control of personal information, as well as intensity and diversity of online activities. As expected, the perceived quality and effectiveness of government regulations is associated with alleviating online privacy concern of internet users. However, this effect is more complex because computer anxiety and desire to maintain control over personal information online showed to be significant variables in our model as well.

Theoretical implication of the research is that items and variables successfully tested in this study could be further used to develop an integrated theoretical framework of online information privacy concerns (as proposed by Li, 2012) and privacy resilience, which is another under-investigated area of human behaviour in the digital age. With an extended set of variables in the model, our findings might provide additional insights for national policy-makers, particularly in the context of the GDPR regulation in force from 2018. The practical implications of our research are seen for developing business strategies, namely companies and managers should clearly communicate their compliance with the privacy regulations to assure customers that their personal data are well-protected and safeguarded. If the perceived effectiveness of the regulatory framework is one of the major determinants of online privacy concern of internet users, i.e., consumers, businesses should take this opportunity and turn it to their competitive advantage.

On the other hand, breaches in privacy protection of data which are collected and used by government agencies could permanently destroy public trust in the national regulatory framework. GDPR is expected to have strong impacts on business but it is too early to tell whether it could also change the attitudes of citizens, consumers and internet users. In this context, the relationship between regulations and online privacy concern calls for further exploration in future research.

This study is not without limitations. A potential source of bias in our model is the response rate to the survey, calculated as the share of fully completed questionnaires in the total number of respondents contacted. It should be emphasised that the denominator of this ratio also includes those who were not qualified to complete our survey (younger than 18 years of age or those who do not use the internet). This raises the issue of whether the people who did not agree to answer questions from the survey were fundamentally equivalent to those who answered the questions.

Although the answer is 'probably not', numerous recent studies point to the fact that the response rate in telephone surveys is not a good indicator of data quality, i.e., the results do not differ significantly with respect to the response rate (e.g., Holbrook, Krosnick & Pfent, 2008). Also, even if bias exists due to a low response rate, it is expected to work downward. Namely, assuming that people who do not want to respond to surveys are fundamentally different from those who agree to respond, those non-respondents are expected to be more concerned about their privacy. Consequently, the existence of this bias means that our estimates refer to the lower limit, or to people who are less concerned about their privacy and thus more willing to respond to the survey. Finally, this analysis could be expanded to other countries by applying the same survey methodology and could provide comparable cross-country insights. Replicating this research in other countries would test if our findings could be considered generally valid in a global digitized world.

Notes

1. The questionnaire is available from the authors upon request.
2. Available at https://www.echr.coe.int/Documents/Convention_ENG.pdf.
3. Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, adopted on January 28, 1981, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.
4. Available at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.
5. Available https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001R0045&from=EN.
6. More information available at https://epic.org/international/eu_privacy_and_electronic_comm.html.
7. More information available at https://epic.org/international/eu_privacy_and_electronic_comm.html.
8. Constitution of the Republic of Croatia, available at http://www.sabor.hr/Default.aspx?art=2405.
9. More information available at http://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet?desktop=true.
10. More information on Croatian Data Protection Agency available at www.azop.hr.
11. More information available athttp://www.cbronline.com/news/cybersecurity/data/european-parliament-approves-general-data-protection-regulation-in-historic-privacy-ruling-4864721.
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.
13. More information available at https://www.eugdpr.org/key-changes.html.
14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

Acknowledgment

This work was supported by the Croatian Science Foundation under Grant number 7913-Extended Model of Online PRIvacy CONcern.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science (New York, N.Y.)*, *347*(6221), 509–514. doi:10.1126/science.aaa1465

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.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316. doi:10.1057/ejis.2012.23

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. doi:10.1287/isre.1060.0080

Dommeyer, C., & Gross, B. (2003). What consumers know and what they do: an investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, *17*(2), 34–51. doi:10.1002/dir.10053

Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management*, *54*(7), 948–957. doi:10.1016/j.im.2017.02.004

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, *133*(1), 111–123. doi:10.1007/s10551-014-2346-x

Henderson, H. (2015). *Online Privacy and Government*. San Diego: Reference Point Press.

Holbrook, A. L., Krosnick, J. A., & Pfent, A. (2008). The causes and consequences of response rates in surveys by the news media and government contractor survey research firms. In J. Lepkowski, C. Tucker, J.M. Brick, E. D. de Leeuw, L. Japec, P. J. Lavrakas, M.W. Link, & R.L. Sangster (Eds.), *Advances in telephone survey methodology* (pp. 499–528). New York, NY: Wiley.

Hoy, G. M., & Milne, G. (2010). Gender differences in privacy-related measures for young adult facebook users. *Journal of Interactive Advertising*, *10*(2), 28–45. doi:10.1080/15252019.2010.10722168

Koops, B.-J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2017). A Typology of Privacy. *University of Pennsylvania Journal of International Law*, *38*(2), 483–575.

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and infor- mation privacy concerns on behavioural intentions. *Journal of Computer Information Systems*, *48*(4), 15–24.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. doi:10.1016/j.dss.2012.06.010

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. doi:10.1007/s11747-006-0003-3

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. doi:10.1287/isre.1040.0032

North, D. (1990). *Institutions, institutional change and economic performance*. Cambridge: Cambridge University Press.

OECD. (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980, available at http://www.oecd.org/document/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring, Individuals' Concerns about Organisational Practices. *MIS Quarterly*, *20*(2), 167–196. doi:10.2307/249477

Parasuraman, S., & Igbaria, M. (1990). An examination of gender differences in the determinants of computer anxiety and attitudes toward microcomputers among managers. *International Journal of Man-Machine Studies*, *32*(3), 327–340. doi:10.1016/S0020-7373(08)80006-5

Peštek, A., Resić, E., & Nožica, M. (2011). Model of Trust in E-Transactions. *Economic Research-Ekonomska Istraživanja*, *24*(3), 131–146. doi:10.1080/1331677X.2011.11517472

Raab, C., & Szekely, I. (2017). Data protection authorities and information technology. *Computer Law & Security Review*, *33*(4), 421–433. doi:10.1016/j.clsr.2017.05.002

Rauhofer, J. (2013). One Step Forward, Two Steps Back?: Critical Observations on the Proposed Reform of the EU Data Protection Framework. *Journal of Law and Economic Regulation*, *6*(1), 57–84.

Reay, I., Beatty, P., Dick, S., & Miller, J. (2011). Do you know where your data is? A study of the effect of enforcement strategies on privacy policies. In H. R. Nemati (Ed.), *Security and Privacy Assurance in Advanced Technologies* (pp. 374–400). Hershey: Information Science Reference.

Rust, R., Kannan, P. K., & Peng, N. (2002). The customer economics of internet privacy. *Journal of Academy of Marketing Science*, *30*(4), 455–464. doi:10.1177/009207002236917

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1016.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36–49. doi:10.1287/isre.13.1.36.97

Thatcher, J. B., & Perrewe, P. L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly*, *26*(4), 381–396. doi:10.2307/4132314

The Surveillance Project (2008). *The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance Summary of Findings*. Kingston: Queen's University.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, *18*(4), 326–348. doi:10.1108/09564230710778128

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. doi:10.17705/1jais.00281

Yeh, C.-H., Wang, Y.-S., Lin, S.-J., Tseng, T.-H., Lin, H.-H., Shih, Y.-W., & Lai, Y.-H. (2018). What drives internet users' willingness to provide personal information? *Online Information Review*, *42*(6), 923–939. doi:10.1108/OIR-09-2016-0264

Zhang, Y., Chen, J., & Wen, K. (2002). Characteristics of internet users and their privacy concerns - a comparative study between China and the United States. *Journal of Internet Commerce*, *1*(2), 1–16. doi:10.1300/J179v01n02_01

Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile commerce and consumer privacy concerns. *Journal of Computer Information Systems*, *53*(4), 31–38. doi:10.1080/08874417.2013.11645648

Zukowski, T., & Brown, I. (2007). Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns. In SAICSIT (Eds.), *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 197–204). ACM New York, NY, USA.

Appendix 1

Regulative framework in the EU and Croatia and the GDPR

Within most European countries, the right to a private life as protected by Article 8 of the European Convention on Human Rights (ECHR)[2] and the data protection laws that eventually developed is ensured both at national and international level. At the EU level, one of the first documents addressing the protection of individual data being automatically processed dates back to 1981[3]. The more detailed EU data protection framework was developed a decade later. That framework includes, among other things, the 1995 Data Protection Directive[4], the 2001 EC Data Protection Regulation governing processing activities by the EU institutions[5], and the 2002 Directive 2002/58 on Privacy and Electronic Communications known as the ePrivacy Directive. The latter aimed to regulate 'online privacy including browsing on the internet,

using a mobile phone, wearables or other internet-connected devices'[6]. The ePrivacy Directive, however, failed to provide efficient safeguards:

'The failure to meet the objectives of the directive is on the one hand due to fragmented implementation across EU member states. On the other hand, the rules have been poorly enforced and lawmakers could not keep up with the pace of development in technology. The law has left users vulnerable to consequences of the extensive usage of smartphone (app)s, online profiling, social media, and the explosion of the internet in general.'[7]

Personal data protection in Croatia is a constitutional category as well:

Article *37*[8]

The safety and secrecy of personal data shall be guaranteed for everyone. Without consent from the person concerned, personal data may be collected, processed, and used only under the conditions specified by law.

Protection of data and oversight of the operations of information systems in the state shall be regulated by law.

The use of personal data contrary to the express purpose of their collection shall be prohibited.

In Croatia, the Personal Data Protection Act (Official Gazette 103/03, 118/06, 41/08, 130/11, 106/12) and by-laws are in accordance with EU regulations, namely with:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of January 28, 1981 and its Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows.

The persistent challenge for EU legislators is to align regulations to the real life situations driven by new ICT usage. Therefore, the Council of Europe is updating its Personal Data Protection Convention – 'Convention 108' – with an aim to address challenges for privacy resulting from the use of new information and communication technologies[9], and the Croatian Data Protection Agency is following the EU directions[10].

The issue of personal information protection is additionally raised in the European Union by introducing the General Data Protection Regulation (GDPR) for EU member states and non-EU based companies operating within the EU. In 2016, when the European Parliament approved the GDPR, it was evaluated as a historic privacy ruling that would impact everyone in this digital world[11]. The aim of the GDPR is to protect all EU citizens from privacy and data breaches. The new regulation on processing and movement of personal data[12] is considered an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the digital single market. According to the new GDPR rules in force from May 2018, businesses will have to comply with various provisions, including 'the right to be forgotten'; 'clear and affirmative consent' to private data processing; the right to know when data has been hacked; and the right to transfer data to another service provider.[13] In practice, this means that citizens will have expanded rights to access data, e.g., to obtain from companies confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. The principle of data portability has been introduced as well to guarantee the right for people to receive the personal data concerning them, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of citizens. Data subjects, in our case internet users, should give clear consent to collect, process, and use their data, and can withdraw the consent. Consequently, they might require erasing their personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. Finally, GDPR legalises a concept of privacy by design (which calls for the inclusion of data protection from the onset of the designing

of systems) and data minimisation. The latter imposes holding and processing only the data absolutely necessary for the completion of duties, as well as limiting the access to personal data to those needing to act out the processing.

GDPR applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU since GDPR applies to the processing of personal data by controllers and processors in the EU[14]. One of the most serious infringements is not having sufficient customer consent to process data or violating the core of privacy by design concepts. Nonetheless, national governments may exclude public institutions from money sanctions in the case of GDPR rules infringements. Currently there is a public debate in Croatia on the Government proposal to exclude public institutions from paying fines if breaching the GDPR rules. This proposal discriminates private vs. public data holders and might raise negative public opinion on the effectiveness of government regulations in protecting privacy.

Appendix 2

Table A1. Definition of five Croatian regions.

Region	County
Zagreb	Zagreb
	City of Zagreb
Western Croatia	Primorje-Gorski Kotar
	Lika-Senj
	Istria
Eastern Croatia	Virovitica-Podravina
	Požega-Slavonia
	Brod-Posavina
	Osijek-Baranja
	Vukovar-Srijem
Central Croatia	Krapina-Zagorje
	Sisak-Moslavina
	Karlovac
	Varaždin
	Koprivnica-Križevci
	Bjelovar-Bilogora
	Međimurje
Southern Croatia	Zadar
	Šibenik-Knin
	Split-Dalmatia
	Dubrovnik-Neretva