The extended model of online privacy concern

; ; ; ; ; ;

The Institute of Economics, Zagreb

PRIvacy CONcern

HRZZ Croatian Science Foundation

The Extended Model of Online Privacy Concern

Ivan-Damir Anić
Jelena Budak
Edo Rajh
Vedran Recher
Vatroslav Škare
Bruno Škrinjarić
Mateo Žokalj

e-ISBN 978-953-6030-50-7

Zagreb, 2018

IZDAVAČ
Ekonomski institut, Zagreb
Trg J. F. Kennedyja 7, Zagreb
http://www.eizg.hr

ZA IZDAVAČA
Maruška Vizek, ravnateljica Ekonomskog instituta, Zagreb

AUTORI
Ivan-Damir Anić
Jelena Budak
Edo Rajh
Vedran Recher
Vatroslav Škare
Bruno Škrinjarić
Mateo Žokalj

AUTORI FOTOGRAFIJA
Branka Domić
Tihana Iviček

LEKTOR
Jelena Mihalj

GLAVNI (IZVRŠNI) UREDNIK
Jelena Mihalj

TEHNIČKI UREDNIK
Goran Rožić

GRAFIČKO OBLIKOVANJE
Endem d.o.o.

e-ISBN 978-953-6030-50-7

This work has been fully supported by the Croatian Science Foundation under the project number 7913. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of Croatian Science Foundation.

CONTENTS

ABOUT THE PRICON PROJECT

The idea of PRICON project was born in 2013 at the team meeting in the Institute of Economics, Zagreb. That was the time when the first round of newly designed calls for proposals for research projects was announced by the Croatian Science Foundation.

Three researchers at the Institute, Ivan-Damir Anić, Jelena Budak and Edo Rajh, at that point already had had track records of working together at the privacy and surveillance issues within the internal research project they conducted since 2011. In the course of that project, as economists-newcomers to that field, mostly reserved to sociologists, philosophers, lawyers and IT experts, they became more and more aware of the gaps in the existing body of knowledge. There was an abundant literature - both theoretical and empirical studies tackling privacy from diverse point of views. However, the big exhaustive model for studying privacy as an indeed complex phenomenon was missing. And still, when talking about privacy today, that is privacy in the digital age, one has to think about privacy when online. Actually, is there any privacy when online, in our everyday life as customers, employers, students…? What do we sense as privacy intrusion, and how much is a person nowadays aware or concerned about privacy intrusion? Do we change our behaviour accordingly? What actions do we take when confronted with online privacy issues? Is privacy of a typical Internet user protected by regulations? Do we trust business privacy protection policy or national regulators? Finally, do people in different societal groups share similar attitudes about online privacy and would they take similar actions? If not, what factors explain the variations? These questions intrigued our research curiosity and stand in the core of the PRICON research project.

Although previous studies have proposed various variables, concepts, and/or tested various theoretical models of antecedents and consequences of online privacy concern, there is no single widespread accepted model of online privacy concern. The extant body of research covering the online privacy theme deals with a limited number of antecedents and consequences, focusing on particular determinants, causes and consequences of either rather narrow or too general online privacy concern aspects. We have identified a lack of a

comprehensive and integrated theoretical framework that would consolidate various streams of research into one model as a missing link in the literature in the online privacy concern field, and PRICON is created to fill that gap.

Extended model of online PRIvacy CONcern (PRICON) is a research project aimed at developing a comprehensive integrated model of privacy concern in the online environment and empirically testing it in order to provide deeper understanding of various interactions between antecedents, concerns and consequences of online privacy. The research objectives were initially achieved by identifying and developing (i) a comprehensive list of antecedents such as demographic factors (e.g. gender, education), experience factors (e.g. internet use experience, web expertise) and social-psychological factors (values, attitudes), and (ii) a comprehensive list of consequences of online privacy concern on individual-user level. These inputs will be used to develop an extended integrated model of online privacy concern in order to examine conceptual interrelations.

The project started July 1, 2014 and ends June 30, 2018. The core research team was formed of senior researchers at the Institute of Economics, Zagreb. Jelena Budak is the principal investigator and project lead, due to her previous experience in the EU funded COST action Living in Surveillance Societies network and leading the internal project Privacy and Surveillance in Western Balkans. Ivan-Damir Anić is a PRICON team member who brought valuable consumer behaviour expertise into the project. Edo Rajh is a PRICON team member specialized in marketing research and survey methodology. We wanted to include into the project the expertize and synergy effects from colleagues coming from other institutions, and Vatroslav Škare from the Faculty of Economics and Business, University of Zagreb joined the team and he brought his knowledge of digital marketing to the benefit of the project. PRICON project was recognized as a great opportunity for young researchers as well, so Bruno Škrinjarić, a young researcher from the Institute of Economics, Zagreb joined the team from the very beginning of the project. PRICON project enabled the project lead Jelena Budak to apply to another Croatian Science Foundation call for supervising the doctoral student and got the financing for one doctoral student at PRICON project. In January 2015,

PRICON project team was finally completed with Vedran Recher, a doctoral student whose dissertation “The impact of privacy concern on consumer behavioural intention in the online environment”, was completed in October 2017.

The project started with an extensive examination of the relevant literature in the field, and in parallel we conducted partial studies to test whether some potential variables should be included in the model as antecedents or consequences of online privacy concern. In the second year of the project, main effort was put into the designing of the PRICON model. The variables and their relations were borrowed from the literature and for each variable in the model an item in the questionnaire was formulated. The process of designing the survey to test the model was carefully performed in several phases, including semi-structured interviews and pilot testing of the survey questionnaire. We were aware that the right design of the model and variables, as well as field research that followed, was crucial for the project. Coordinating and monitoring this phase of the PRICON project required thorough documenting of every step we made. Therefore, we came up with the idea to put all our work in a more structured and written form and that is how our PRICON book was born.

Chapters of the book resemble the phases of the project, and although the entire team participated in all phases, some of us were more involved or more familiar with selected activities, so these members appear as authors of associated chapters. The aim of the book is to document our work that might be a helpful guide for other researchers engaged in similar projects. Recording our activities in this way should help us in future publishing of PRICON results as well, if and when we would need to recall, for example, the details on the methodology applied. In the course of the project, research papers were produced, submitted for publication, or published, and included in the book as reprints, or in preliminary versions, such as working materials. As the PRICON project evolved, cooperation with other academics and students developed so naturally, and at the end of the official project duration, we have several co-authored papers and many friends and colleagues in our network. However, the most important motif for us was to make an extra effort in bringing together our expertise and to produce a publication that will outlive the project. In that way, we would thank the

Croatian Science Foundation for its support to this research.

The PRICON team appreciates much the assistance of Tihana Iviček and Jelena Mihalj, our project coordinators who took care of all administration associated with management of such a complex project. Finally, the PRICON project and this book would not be possible without the institutional support we received from the Institute of Economics, Zagreb. We would like to thank our colleagues for their unconditional belief in our project.

ABOUT US

The PRICON team 2014

By Tihana Iviček.

Team members (from left to the right) are Bruno, Edo, Vatroslav, Jelena, Vedran and Ivan-Damir.

Bruno Škrinjarić, is a research assistant at the Institute of Economics, Zagreb since 2011. His research interests are economics of education, applied econometrics, and development of key competencies. His engagement at the PRICON project refers to the survey methodology in part of semi-structured interviews and valuable contribution in including and exploring personality traits as determinants of privacy concern. Bruno is a PhD student at the University of Ljubljana.

Edo Rajh is a senior research fellow at the Institute of Economics, Zagreb, the Department for Innovation, Business Economics and Business Sectors and a team member researcher in the PRICON project. His primary research areas are market research methodology and measurement scales development and this expertize he successfully applied to the PRICON project.

Vatroslav Škare is an assistant professor at the Marketing Department atthe Faculty of Economics and Business, University of Zagreb. His research interests are services marketing, services innovation, digital marketing, brand and country image. Vatroslav contributed to the PRICON project with adding the marketing business approach to studying people's behaviour.

Jelena Budak is a senior research fellow at the Institute of Economics, Zagreb. Her research interests are institutions and applied institutional analysis, public attitudes and privacy issues in transition economies. She is a lead of the PRICON project.

Vedran Recher is a PhD student at the Institute of Economics, Zagreb, engaged with the PRICON project. In his dissertation, Vedran focused on how online privacy concern affects consumers' intentions to transact. His research interests are behavioural economics along with their application to privacy issues.

Ivan-Damir Anić is a senior research fellow at the Institute of Economics, Zagreb. His main research interests are consumer behaviour and marketing. As a member of the PRICON team, Ivan-Damir contributed to the project with extensive literature review of the privacy in commercial setting and by designing questionnaire items in this field.

1. PRIVACY DEFINITION AND LITERATURE OVERVIEW

1.1. Privacy and privacy interpretation

When mentioning privacy, it seems that everyone knows what that term means. But when one starts talking about the privacy, it turns out that for each individual, privacy represents something different, although similar. Notion of privacy, therefore, differs from person to person. It is not surprising that the concept of privacy is viewed in different ways in different situations. In studying privacy, the context and approach is distinguished by science fields and professions, and in recent years the privacy research is mostly interdisciplinary.

Privacy is a vague concept. The narrower definition developed and used by European scholars is that privacy is a personal space under the exclusive control of the individual, so an individual can determine the extent to which data about him/her is being collected and used ("informational self-determination"). Under the current notion of privacy as a personal issue, the usage of personal information is adequately protected and should be supported by newly developed institutional mechanisms (Stalder, 2002). Today, legislation and policy-makers recognize the social value of privacy. Law regulations for data protection and privacy are developed in many countries, so privacy protection became a matter of public policy all across the world. Perceptions of privacy violations can be very subjective and therefore difficult to be legally defined and protected; especially when it comes to implementation (Benett, 2011). The policy makers have demanding task to balance individual needs for privacy with society requirements (Zureik, 2004). Empirical and legal studies of privacy are exploring the importance of privacy, awareness of how private/public sectors are protecting privacy; reaction to specific privacy protection measures; privacy and national security relationship and harmonization of privacy standards (Zureik, 2004).

For economists, privacy is still not in the core focus of their research, but in the near future one could envisage a larger number of economic studies on privacy to emerge, such as cost and benefit analysis of privacy protection. Privacy Impact Assessment (PIA) is seriously

considered by the regulatory authorities of the European Commission (Wright and de Hert, (Eds.), 2012). Effect of privacy concern in business transactions has been regularly assessed, for example in the analyses of companies trading over the Internet. Companies, in particular in the ICT sector, have built privacy policy in their products and services, developing in parallel sophisticated mechanisms to collect private data from their clients. In the digital age, privacy is a commodity market and a big business.

In modelling the privacy concern online, we start from a brief literature review in the field of general privacy. The definitions of privacy and of privacy online serve as an introduction to the literature review we used in our research on online privacy. Finally, this chapter brings abstracts of two major theory and review papers on information privacy research. Smith, Dinev, and Xu (2011) provided an interdisciplinary review, and Pavlou (2011) discussed the state of the literature and directions of the information privacy multidisciplinary studies in the future.

1.2. General privacy literature

Warren and Brandeis (1890) were one of the first to define privacy in discussion about the invasion of privacy by the media at the turn of 19th century. They offered a broad definition of privacy as a right to be ‘’let alone” in a sense of one’s right to ‘’keep his private life”. This conventional concept of privacy is incorporated into private protection legislation in Anglo-Saxon societies (for brief introduction to legal evolution of the right to privacy in the US see Henderson, 2015).

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). This concept of privacy is prevalent in European privacy policy. Information privacy served as a basis to establish so called “fair information practices” and was used in designing data protection legislation in number of countries. The privacy rights should be balanced with the state’s legitimate need for information. However, personal information collected by the state and private companies

is shared beyond the knowledge and control of individuals concerned. Some concepts are seen as too narrow, such as a concept of privacy defined in terms of intimacy only (Inness, 1996).

Buchanan et al. (2007) emphasize different dimensions of privacy from the literature (Burgoon et al. (1989) and DeCew (1997)) and their intertwinement: (i) informational privacy is defined as individual's right to determine how, when, and to what extent information about the self will be released to third party, (ii) accessibility privacy overlaps with informational privacy in cases where ''acquisition or attempted acquisition of information involves gaining access to an individual", but it also extends to cases where physical access is at stake, which also overlaps with Burgoon's (iii) physical dimension of privacy defined as the degree to which a person is physically accessible to others, (iv) expressive privacy which ''protects a realm for expressing ones self-identity or personhood through speech or activity and (v) social/ communicational dimension of privacy, which is an individual's ability and effort to control social contacts (Altman, 1975). Tavani (2008, 2010) offers somewhat different distinction of privacy dimensions and divides them into (i) informational privacy, (ii) physical/accessibility privacy, (iii) decisional privacy and (iv) psychological or mental privacy (cited in Fuchs, 2012).

Fuchs (2012) distinguishes between three different theories of privacy. In a control theory of privacy, there is privacy if one chooses to disclose all personal information about oneself. In an absolute restricted access theory of privacy, there is privacy only if one lives in solitary confinement without contacts to others. The third, i.e. the restricted access/limited control theory (RALC) of privacy tries to combine the former two concepts.

Etzioni (1999) stresses that privacy can undermine common goods and that privacy is not automatically a positive value. It promotes an individual agenda and possessive individualism that can harm the common good. Fuchs (2012) argues that the question is not how privacy can be best protected, but whose privacy should be protected in which cases, and in which cases not.

He argues that anonymity of wealth, high incomes and profits makes income and wealth gaps between the rich and the poor invisible, and thereby ideologically helps legitimatizing and upholding these gaps. It can therefore be considered an ideological mechanism that helps reproducing and deepening inequality. Furthermore, he states ‘’Privacy under capitalism can best be characterized as an antagonistic value that is on the one side upheld as a universal value for protecting private property, but is at the same time permanently undermined by corporate surveillance into the lives of humans for profit purposes. Capitalism protects privacy for the rich and companies, but at the same time legitimates privacy violations of consumers and citizens. It thereby undermines its own positing of privacy as universal value.” Fuchs (2012:141.) He emphasizes the distinction between liberal and socialist concept of privacy. He argues that liberal concept of privacy, i.e. privacy as individual right, protects the rich and the accumulation of wealth away from public knowledge. He labels liberal privacy theory as ‘’privacy fetishism”, because it emphasizes only positive values such as autonomy, counterculture, creativity, democracy, eccentricity, dignity, freedom, friendship, human relationships, imagination, independence, etc. These analyses tend not to engage with possible negative effects of privacy such as exploitation and income and wealth inequality. Instead of this conception of privacy, Fuchs (2012) advocates socialist conception of privacy that tries to strengthen the protection of consumers and citizens from corporate surveillance. Therefore, economic privacy is posited as undesirable in those cases where it protects the rich and capital from public accountability, but as desirable where it tries to protect citizens from corporate surveillance. He supports historical approach to the privacy issues since privacy is not an anthropological need, but a socially created need that varies historically (Moore, 1984).

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 behaviour, including wiretapping, surreptitiousness, 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 data bases.

The concept of privacy has also been described through its various dimensions. The approaches may vary depending on the context of studying privacy issues across disciplines. Thus, Clarke (1999; 2009) distinguishes between four dimensions of privacy: (i) privacy of the person, concerned with the integrity of the individual's body, (ii) privacy of personal behaviour, sometimes referred to as 'media privacy', which concerns sexual preferences and habits, political activities and religious practices, (iii) privacy of personal communications which contains the freedom to communicate without routine monitoring of their communications by third persons and (iv) privacy of personal data which covers the issue of making the data about individuals automatically available to third parties; individuals must be able to exercise a substantial degree of control over the data about themselves and its use. Clarke (2006) also emphasizes the notion of 'private space' which is, he argues, vital to all aspects of behaviour, and is relevant in 'private places' such as the home and toilet cubicle, as well as in 'public places', where casual observation by the few people in the vicinity is very different from systematic observation and recording of images and sounds.

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, 2012), and a political value. In a modern society, privacy is recognized as individual right, but also as a social and political value (Raab and 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". Solove (2006) identifies four principal groups of ''socially recognized privacy violations" as follows: (i) information collection, i.e. the way data is gathered – surveillance, interrogation, (ii) information processing, i.e. storing, analysis and manipulation of data – aggregation, identification, insecurity, secondary use of information and exclusion, (iii) information dissemination – breach of confidentiality, disclosure, exposure, increased accessibility,

blackmail, appropriation of someone's identity, defamation before the public in false light and (iv) invasions – intrusion into someone's private sphere and decisional interference which is connected to information privacy. Raab and Goold (2011) provide an example for a case when privacy is recognized as ability to control information; then (un)fair information practices will be seen as a major privacy concern. The privacy rights should be balanced with the state's legitimate need for information. However, personal information collected by the state and private companies is shared beyond the knowledge and control of individuals concerned. Increased demand for information and the spread of new technologies such as surveillance cameras indeed limit the purely private spaces. Solove (2008b) exhibits a pyramid concept of data abuse. He 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 are the data protected.

Nowadays, both state and private sector are holding, processing and sharing a large amount of personal information. As the level of surveillance in society increases (including dataveillance), it is becoming more difficult for individuals to protect their identities. Goold (2010) examines the effects of surveillance on the functioning of the rule of law. He argues that citizens would demand for less surveillance when perceiving state surveillance as a threat to political rights and democracy.

Issues relating to privacy and surveillance are gaining in importance across disciplines and have become heatedly contested political issues (Haggerty and Ericson, 2006). Security issues and the associated necessity of enhanced surveillance are subjects of debates among scholars and practitioners (Dinev et al., 2005). New technology-based surveillance practices are being developed to meet the demands for safety, security, efficiency and coordination in the society, but they also introduced certain threats. Many people have become deeply concerned about the spread of surveillance (Dinev et al. 2005; Goold, 2009). In a 'surveillance society', institutions and government might gain too much power over individuals. Data

protection, which is closely related to privacy and surveillance, has also become one of the major concerns of modern society (Solove, 2008a). Not only can awareness of surveillance, security and data protection issues make a person feel uncomfortable, it can also cause people to alter their behaviour (Solove, 2006). Understanding the effects of privacy concern and the issues of surveillance, security and data protection, as well as addressing the multi-dimensional impacts they have on individuals and society, has become a part of research agenda in many countries.

Past research examines privacy from various perspectives, including meaning of privacy, general privacy concern, public opinion trends, the impact of surveillance technologies, causes and consequences of privacy protection, consumers' responses to privacy concern, and the need for government surveillance and privacy regulation (e.g. Patton, 2000; Kumaraguru and Cranor, 2006; Goold, 2009; Wirtz et al., 2007). Previous studies indicate that there are differences in information privacy concerns across cultures (Dinev et al., 2005; Ur and Wang, 2013; Chiou, Chen, and Bisset, 2009), and that different groups of people share different views on surveillance and privacy as well (Haggerty and Gazso, 2005; Wirtz et al., 2007). Citizens' attitudes towards privacy and data protection also vary according to demographic characteristics (e.g. European Commission, 2011). Additional attitudinal studies of privacy, data protection, surveillance and security would help to understand people's behaviour, and different behaviour requires different policy approaches (Wirtz et al., 2007). Gellman and Dixon (2011) stress the importance of the intertwinement of online and offline privacy issues. As they note, ''online and offline privacy issues cannot be separated completely, nor should they be. What happens offline affects what is done online and vice versa" (Gellman and Dixon, 2011: xii); and here it comes to our next definition of what privacy online means.

1.3. Privacy online

Under Article 8 of the Charter of Fundamental Rights of the EU, a right to protection against the collection and use of personal data forms a part of the right to respect for private and family life, home and correspondence (European Union Agency for Fundamental Rights, 2014). When we dispute the issues of online data protection, it is important to have the

explicit definition of the subject, i.e. personal data. European Union Agency for Fundamental Rights (2014: 36) defines personal data:

“Data are personal data if they relate to an identified or at least identifiable person, the data subject. A person is identifiable if additional information can be obtained without unreasonable effort, allowing the identification of the data subject. Authentication means proving that a certain person possesses a certain identity and/or is authorized to carry out certain activities.”

The Oxford dictionary defines “online” as “controlled by or connected to a computer” and as an activity or service which is “available on or performed using the Internet or other computer network”.

In the early 1990s online meant what is now considered to be the old-fashioned Internet (Gellman and Dixon, 2011). The Internet in that time had far narrower scope than today. Instead of Web pages, users surfed bulletin boards, Usenet discussion groups, and pre-websites called Gophers (Gellman and Dixon, 2011). Today, online means connections to the Internet in very broad terms and in its most technical sense refers to computers or devices that connect to the Internet and the World Wide Web (Gellman and Dixon, 2011).

As boundaries of online privacy are changing as rapidly as technology, it is hard to establish a firm concept of what online privacy should be (Gellman and Dixon, 2011). Online privacy has a different dynamic than offline privacy, because online activities do not respect traditional national or conceptual borders. According to Gellman and Dixon (2011), online has a greater capacity for ‘’memory” via longer retention of and easier access to information. They describe extensively the chronology of online privacy in the fourth chapter of their book, and argue that online privacy relates only to online activities, and although this may seem like a limited sphere of privacy, that may not be the case for teenagers who have grown up with the Internet as a presence throughout their entire lives, i.e. they are ‘’digital natives” (Reed, 2014).

As Allen (2015) argues, before the penetration of the Internet and ‘’online life”, maintaining privacy and securing personal information meant keeping important documents and financial material locked away in a safety deposit box or home safe, but nowadays information about almost every aspect of a person’s life is electronically available and therefore vulnerable to computer hackers. Walther (2011) distinguishes three complicating factors that confront the users of online systems: (i) a misplaced presumption that online behaviour is private, (ii) that nature of the Internet at a mechanical level is quite incommensurate with privacy and (iii) that one’s expectation of privacy does not constitute privileged communication by definition. Furthermore, many Internet users fail to realize that something once put online, more or less stays online and may be retrieved by others and replicated, despite the subsequent inclination or efforts of the original poster to remove it (Walther, 2011:4).

Pauxtis and White (2009) warn that privacy and general consumer protection on the Internet is no longer limited to the safeguarding of personal financial information, such as credit card numbers. Instead, a vast amount of personal information is being given out every day by using any major search engine. For example, Google logs much of what their users search for and then use that information to their advantage. Salehnia (2002) defines Internet privacy as ‘’the seclusion and freedom from unauthorized intrusion”. Pauxtis and White (2009) give an example of this concept in the real-world. End-user who utilizes Google several times a day may come to find out three years later that every search they have ever made was logged, time - stamped, and potentially used to Google’s own business benefit. This is an illustration of ‘’unauthorized intrusion” which is happening millions of times a day.

With the spread of the Internet, more and more studies conceptualize and explore online privacy concern, which is considered to be a subset of consumer information privacy. In a digital era, the meaning of privacy has evolved and now focuses on personal information shared with family, friends, businesses, and strangers, while consumers must actively participate in self-protection as new digital technologies might be harmful for them (Markos, Labrecque, and Milne, 2012). Online privacy involves the rights of an individual concerning the storing, reusing, provision of personal information to third parties, and displaying of

information pertaining to oneself on the Internet. The invasion of privacy on the Internet includes the unauthorized collection, disclosure or other use of personal information (Wang, Lee, and Wang 1998). The conceptualizations and measurement of online privacy concern construct differ significantly across studies, and yet the constructs of privacy concern share some common items and dimensions (Li, 2011). There are also two approaches to examine privacy concern: online privacy concern in general e-commerce environment and website-specific privacy concern (Li, 2014).

Online privacy literature at the first place deals with the problem of how to measure privacy concern of Internet users. Based on their survey and analysis, Buchanan et al. (2007) suggested three scales for measuring the level of online privacy concern: one general, called 'privacy concern' which is defined through people's attitude towards privacy, and two behavioural, ''general caution" and ''technical protection" which concerns people's demeanor with regards to protection of their privacy. Their proposed measure contains sixteen items that capture specific privacy issues such as identity theft, access to medical records, virus attack, and mishandling of e-mails. Metzger and Docter (2003) suggest that online privacy concern includes the following dimensions: anonymity, intrusion (e.g., spam, data mining), surveillance and autonomy. Malhotra, Kim, and Agarwal (2004) developed the measure for information privacy concern for online consumers, which includes the following dimensions: the control over personal information, awareness of privacy practices and data collection. Dinev and Hart (2004) proposed the following two dimensions for Internet privacy concerns: abuse of personal information and information finding. Several studies used broader concept of privacy concern (Korgaonkar and Wolin, 1999; Krohn, Luo, and Hsu, 2002), which includes Internet users' privacy concerns about their financial transactions on the web, distribution of personal financial data, web intrusion, the control over unwanted messages and widespread availability of personal information on the Internet.

Smith, Milberg, and Burke (1996) developed the Concern for Information Privacy (CFIP) Scale. It identified four factors: collection, errors, secondary use and unauthorized access to information as dimensions of an individual's concern for privacy (cited in Buchanan et

al. (2007)). Malhotra, Kim, and Agarwal (2004) operationalized multidimensional notion of Internet Users Information Privacy Concerns (IUIPC), which recognizes multiple aspects of informational privacy. They identify attitudes towards the collection of personal information, control over personal information; and awareness of privacy practices of companies gathering personal information as being components of a second-order construct they label IUIPC (cited in Buchanan et al. (2007)).

Ur and Wang (2013) suggest a framework for evaluating the extent to which social networking sites' privacy options are offered and communicated in a manner that supports diverse users from around the world. Although their focus is primarily on cross-cultural research of the social media, the proposed framework could be useful for the examination of general cross-cultural online privacy concern. They divide their framework into three aspects: (i) cultural norms, (ii) legal issues and (iii) user expectations. Cultural norms refer to differences between cultures in photo sharing, information revelation, pseudonyms, network structure, communication patterns and technology adoption. Legal issues are mainly related to differences between countries with regards to legal approach to the issue of online privacy. User expectations refer to differences in a user's goals for a particular service, trust in institutions, localized networks and language. 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 would lead to defensive measures to reduce their dependence on these power-holders. Ziesak (2012) studies a link between different types of data collection, different use purposes and concerns for information privacy in the context of personalization. He shows that privacy concerns increase when online merchant informs users about gathering personal and/or behavioural information about its customers. Therefore, the attempt to lower privacy concerns by informing users has provoked a contrary effect. Lewis (2011) stresses the fact that in the voluminous literature on online privacy there have been remarkably few studies on the topic of online privacy behaviour. He includes three behaviour

dynamics in his model: (i) exogenous mechanisms, (ii) associational mechanisms and (iii) structural mechanisms. Yao (2011) and Gurung and Jain (2009) posit that the protection of privacy may be either passive or active. Passive protection involves reliance on government or other external entities, and it is beyond the direct control of one individual. Furthermore, it is dependent on collective actions and institutional support as well as on cultural and sociopolitical norms. On the other hand, active protection relies on individuals themselves actively adopting various protective strategies.

Hartmann (2011) was one of the first to acknowledge the connection between mobility and privacy. He argues that they are moving in different directions, mobility is on the rise, while privacy is diminishing. Furthermore, he writes that the easiest connection between mobilities and privacy is the right to privacy as a pre-condition for public life, to which the mobile context simply adds an additional emphasis. Somewhat more complicated is the right to privacy as something that needs to be created or sustained. In mobile contexts, different kinds of privacy might be observable and necessary depending on the movement and the related location.

Bonneau and Preibusch (2010) conducted a thorough analysis of the market for privacy practices and policies in online social networks. They have found strong evidence that the social networking market is failing to provide users with adequate privacy control. Furthermore, they argue that the market is still in an early stage of aggressive competition for users. These results suggest that the application of utility maximization theory fails to capture all intricacies of the market for privacy in social networking, as experimental economics is suggesting. They found compelling evidence that a major problem is the lack of accessible information for users. Reducing information asymmetry is an important first step towards helping users in making more informed privacy choices (Bonneau and Preibusch, 2010).

Lilien and Bhargava (2009) emphasize the importance of trust in online transactions and argue that privacy and trust can be in a symbiotic or in an adversarial relationship. They focus on adversarial relationship, while they describe the symbiotic one as the situation

when a better privacy provided by a commercial Web site results in its customers' higher degree of trust. In adversarial relationship there is a trade-off between privacy disclosure and trust. For example, when buying online, people provide digital credentials of their credit cards, which reduces the privacy of their owner, but enhances the trust of the other side in the transaction. Rea and Chen (2009) also refer to the impact of trust in e-commerce. They argue that if e-businesses want to collect viable data in order to improve their online offerings and remain competitive, they must (i) implement an accessible and easy-to-read privacy statement and (ii) obtain endorsement from well-known privacy groups, as well as prominently display the resulting certification logo. Wang and Emurian (2005) explored online trust as one of "the most formidable barriers to people for engaging in e-commerce, involving transactions in which financial and personal information is submitted to merchants via the Internet." In a number of studies, trust has been viewed as a mediator between information privacy and willingness to disclose information (Dinev and Hart, 2006). In other studies, authors see trust as an antecedent of privacy (Bélanger, Hiller, and Smith, 2002; Eastlick, Lotz, and Warrington, 2006). Trust as a consequence of information privacy was argued by Malhotra, Kim, and Agarwal (2004) and by Bansal, Zahedi, and Gefen (2010) for health records. On the consequences side of the model, Bansal, Zahedi, and Gefen (2008) see trust as a moderator of the effects of information privacy on behaviour. When it comes to the online consumer behaviour, the effect of trust seems to be stronger in comparison to the effects of information privacy concern.

Hsu (2009) distinguishes adversarial and situational paradigm of privacy. Adversarial one encompasses ignorance of online environments and studying the determinants of privacy (what kind of persons are concerned more about their privacy). She argues that with this approach the determinants fail to explain why users asserting to have higher privacy concerns still disclose sensitive information. She emphasizes the fact that the findings of the literature on privacy concerns focusing on demographics are usually in conflict with each other, which suggests that privacy concerns are not static, but vary with context. Situational paradigm takes two things into consideration: (i) the context of privacy risks and data subjects and (ii) necessity to distinguish privacy concerns from privacy practices. Contexts might be

technology, Web sites' performance, privacy regulations, political system, culture and so on.

To conclude with the privacy online literature, Gurung and Jain (2009) give broad literature overview of research on online privacy and propose an integrative framework of online privacy protection. An individual's trust in online companies and their data collection procedures has been the major factor hindering the growth of electronic commerce (Bélanger, Hiller, and Smith, 2002; (Liu et al. 2004, cited in Gurung and Jain, 2009: 151-152)). Research has also shown that privacy concerns act as a hindrance to the growth of electronic commerce as well (Hoffman, Novak, and Peraltsa, 1999; Miyazaki and Fernandez, 2001). Companies have realized that protecting consumers' private information is an essential component in winning the trust of the consumers and is a must in facilitating business transactions (Bélanger, Hiller, and Smith, 2002; McKnight and Chervany, 2001). There is not enough evidence to prove whether privacy policies are effective in alleviating the consumers' privacy concerns. In the absence of any strong mechanisms, technologies or policies that ensure information privacy, consumers adopt different strategies for their privacy protection. Such strategies may include abstaining from purchasing, falsifying information, and adjusting security and privacy settings in the Web browsers (Chen and Rea, 2004). Gurung and Jain (2009) list the suggested privacy typologies: privacy aware, privacy active, privacy suspicious (Drennan, Mort, and Previte, 2006). Privacy aware refers to being knowledgeable and sensitive about risks associated with sharing personal information online. The privacy active factor refers to active behaviours adopted by consumers in regards to their privacy concerns. Privacy suspicious factor refers to concerns about company behaviour regarding privacy practices (Table 1). However, as privacy is an immensely complex issue, there are many different typologies of privacy attitudes and behaviour.

Table 1. Mixed typology of privacy concerns

Fundamentalists and privacy aware	Fundamentalists and privacy active	Fundamentalists and privacy suspicious
Unconcerned and privacy aware	Unconcerned only	Unconcerned only
Pragmatists and privacy aware	Pragmatists and privacy active	Pragmatists and privacy suspicious

Source: Gurung and Jain (2009: 157)

Privacy controls are defined as consumers' ability to hold control over an unwanted presence in the environment ((Goodwin, 1991) cited in (Gurung and Jain, 2009)). Gurung and Jain (2009) give a non-exhaustive list of variables considered to be the antecedents of online privacy protection behaviour that have been researched in the past. We will revert to the variables later in the context of modelling PRICON, and first proceed with the consumer privacy and privacy issues in the commercial settings.

1.4. Information privacy research consolidated

"The information age has rendered information privacy a core topic in information systems research" Pavlou (2011:977). This chapter brings abstracts of two major theory and review papers on information privacy research published in 2011 in MIS Quarterly. In this issue, Smith, Dinev, and Xu (2011) provided an interdisciplinary review of privacy-related research, and Bélanger and Crossler (2011) provided an in-depth review of existing literature on the information privacy research in the information systems. Based on their critical assessments, Pavlou (2011) discussed the state of the literature and directions of the information privacy multidisciplinary studies in the future. Information privacy refers to a concept of controlling how personal information is collected and used. In the information age, the importance of privacy increased in theory and practice. The abundant body of the theoretical and practical studies of the information privacy in information systems developed, yet Pavlou (2011)

elaborates how more multidisciplinary research is needed and here PRICON fills the gap.

Information privacy is such a complex concept that there have to be studies from many perspectives other than economic: legal, marketing, management, and information systems. The information age exacerbated concerns about information privacy, and Internet made personal information easy to collect, store, process, and use by multiple parties. In return, information technologies developed technical solutions to mitigate information privacy concern.

Since the 1990s, the information privacy has been in focus of the e-commerce and marketing strategies towards consumers where websites want to collect consumer information, and consumers often view this practice as a privacy invasion. Information privacy concerns present a significant obstacle to people engaging in e-commerce (Wang and Emurian, 2005; Pavlou and Fygenson, 2006).

Bélanger and Crossler (2011) provided an in-depth critical review of the existing literature on the information privacy research in the information systems. In the digital era, one cannot easily draw a line between data privacy and communication privacy as argued by Clarke (1999), so Bélanger and Crossler (2011) suggest merging these two categories into all-encompassing information privacy. They however, distinguish the effects of information privacy concerns in the form of intentions and attitudes. The wide range of attitudes makes it difficult to have a coherent stream in the literature. When it comes to behaviour (Bélanger and Crossler (2011) do not differentiate attitudes and behaviour) it seems that information privacy concerns no longer prove to affect an individual's willingness to disclose personal information. They argue that privacy attitudes in the context of RFID (Radio-Frequency IDentification) technology should be more explored in the future, but do not refer to particular studies missing in the area of online privacy. In the systematization of the past research on information privacy tools one could distinguish privacy invasive technologies from privacy enhancing technologies, and this angle is taken mostly by computer scientists. Studies on information privacy concerns, practices and attitudes (that are in the core of the PRICON

model) have, according to Bélanger and Crossler (2011), several key characteristics.

First, most studies are conducted on student population, and in the USA. Accordingly, there is little knowledge on information privacy differences across countries that might be generalized across individuals. Second, studies are mostly conducted at the individual level, so group, organizational and societal aspects are missing. The multilevel model developed by Bélanger and Crossler (2011) suggests that individuals' information privacy concerns are influenced by external factors, such as individual differences. Several individual differences have been studied in prior research, such as gender, age, and education. Other individual differences could be studied, such as the effects of self-efficacy or personality traits like amicability on information privacy concerns. There is also the need to study the moderating effects these individual differences could have on the linkages between information privacy concerns and dependent variables like e-business adoption. To conclude, more studies on information privacy concerns across individuals and information privacy practices are needed in multiple countries other than the U.S., using preferably non-student population.

Information privacy concerns are usually measured in the information systems literature using self-reported scales, as we also employ in PRICON research. There is a general consensus in the literature that information privacy concern corresponds to a person's willingness to render personal information (Dinev and Hart, 2006), to transaction activity (Pavlou, Liang, and Xue, 2007) and to government regulation (Milberg, Smith, and Burke, 2000). To these scales, researchers added many measurements and variables in modelling different dimensions of information privacy concerns. Studies have examined the effects of information privacy concerns as well. Smith, Dinev, and Xu (2011) analysed the information privacy literature from three aspects. The first one considers the conceptualization of information privacy, where they concluded there was no single concept of information privacy that crosses all disciplines, as previously elaborated in this chapter. Secondly, one has to clearly distinguish the concept of information privacy from the similar and related constructs such as anonymity and security. Authors then proceeded with the systematization of information privacy relations to other concepts, where trust often appears as a mediator between information privacy

and willingness to disclose information. They conclude that reducing information privacy concerns correlates with trust, albeit the direct relationship is not generally confirmed.

Smith, Dinev, and Xu (2011) explain two interesting concepts found in the information privacy literature: privacy paradox and privacy calculus. Privacy paradox is a phenomenon where an individual expresses strong privacy concerns and behaves in a contradictory way, for example shares personal information despite proclaimed privacy concerns. It might be associated with the perceived benefits i.e. trade-off between privacy concerns "costs" and "benefits" in a form of service obtained, so called privacy calculus. These two concepts are in particular interesting for economic approach to the privacy concern problem. Economists assume that rational users are willing to disclose personal information in exchange for benefits, but will keep information unrevealed if they see no benefits in return. These studies are abundant in the marketing literature. Privacy of clients and customers i.e. of Internet users observed within PRICON research is invaded by an excessive use of personal information, by the improper use of personal information and by hidden (undisclosed) use of personal information. Related information risk perceived as a potential loss associated with personal information misuse (Featherman and Pavlou, 2003) is studied as an antecedent of information privacy concern (Dinev and Hart, 2006). When weighting potential benefits and losses of disclosing personal information, people think of three types of information privacy benefits: financial rewards, personalization and social adjustment benefits, where personal benefits are less valuated by consumers with high levels of privacy concern (Awad and Krishnan, 2006). Here it comes to the level of analysis, which is, as previously mentioned, predominately at the individual level, followed by the societal level, and significantly less at the group and organizational level (Smith, Dinev, and Xu, 2011).

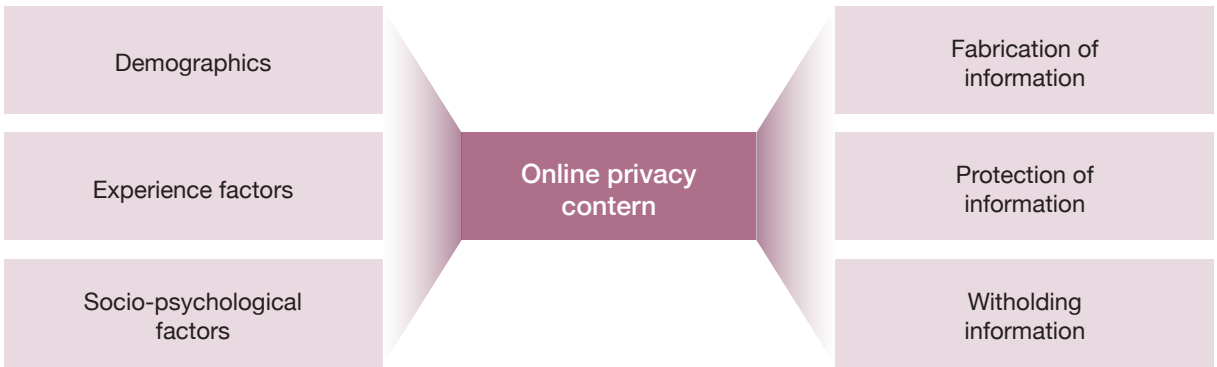
Derived recommendations are to move beyond the individual level of analysis, to utilize a broader diversity of sample populations, to conduct more studies investigating the "why" instead of "how" related to privacy, and to justify the use of existing construct measurements as well as develop more common measurements to be used across studies that in turn will make results comparative and findings more general. Out of these suggested lines of the

future research, all except the first one apply to our PRICON research. Besides advising analytical levels other than individual ones, "empirically descriptive studies have the potential to add value to the literature" (Pavlou, 2011:982). Smith, Dinev, and Xu (2011:1008) argue that "positivist privacy researchers should keep their eye on an optimized Antecedents -> Privacy Concern -> Outcomes macro model that eventually includes an expanded set of antecedents as well as an exhaustive set of outcomes. The ultimate objective should be a macro model that will prove useful across disciplines and contexts", and here PRICON research filled the gap.

2. MODEL

The main goal of PRICON project was to develop a comprehensive and integrated model of privacy concern in the online environment and to empirically test it in order to provide deeper understanding of various interactions between antecedents, concerns and consequences of online privacy. Accordingly, the research objectives were to identify a comprehensive list of antecedents, such as demographic factors (e.g. gender, education, age, employment status, income), experience factors (e.g. internet use experience, web expertise, computer literacy,) and soco-psychological factors (values, attitudes and other "soft" determinants), as well as a comprehensive list of consequences of online privacy concern on individual-user level. Preliminary consequences to be examined encompassed fabrication, protection and willingness to provide personal information online or to withhold it. The multilevel and multidimensional structure of the model was envisioned to reflect the complexity of determinants-dimensions of the privacy concern-consequences nexus. The basic model presented in the PRICON project application reflected the concept of the research. The central variable is online privacy concern, on the left side there is a list of determinants i.e. antecedents, and on the right side of the model are variables representing consequences of online privacy concern (Figure 1).

Figure 1. Conceptual mode of research



2.1. Online privacy concern as a central variable

Online privacy concern is the central variable in our PRICON model. It reflects the level of concern felt by an individual when using the Internet. The intensity or range of online privacy concern is hard to measure and it is highly subjective. Actually, our objective was to measure subjective notion of concern and here we borrowed from the existing literature measurement scales and adapted them for an online environment. The most instructive approach was developed as Global Information Privacy Concern by Smith, Milberg, and Burke (1996). It has been described in Malhotra, Kim, and Agarwal (2004) as a tool "to measure individuals' concerns about information privacy"...that "practitioners have often used a one-dimensional global information privacy concern". Internet is one of the key external drivers of customer privacy concern. Compared to the usage of traditional media in the past, consumers became more alert to information privacy issues when online (Kumar and Reinartz, 2012:283).

Past research identified a number of different antecedents to online privacy concerns, including user-level antecedents that are the focus of our research (see for example Graeff and Harmon, 2002; Dommeyer and Gross, 2003; Yao, Rice, and Wallis, 2007). In general, there are three broad categories of user-level antecedents: demographic factors (e.g. gender, education), experience factors (e.g. internet use, web expertise) and socio-psychological factors (e.g. the psychological need for privacy, generalized self-efficacy, belief in privacy rights). Bearing in mind that privacy in an online context refers to "the rights and interests of an individual that apply to the processing of the information obtained from or about that individual" (Gellman and Dickson, 2011:268), and that advances in IT pose multifaceted challenges to data usage and security (Nemati, 2011), we are led to think of the cultural heritage that shapes our understanding of privacy rights and interests as well. The level of online privacy concern shapes our behaviour on the Internet and beyond. Online privacy concern is expected to alter protective behaviour of an internet user who decides to withhold, fabricate or additionally protect his/hers information. The online privacy concern might influence adoption of new technologies, future usage of online services, and other

types of behaviour, for example sharing private information online. In developing the model we soon became aware that our model is not purely an economic research model but also a socio-economic one (Table 2).

Table 2. Determinants and consequences of online privacy concern

Antecedents / determinants		Consequences (behaviour / attitudes)
Demographics		Protective behaviour: - withholding information - fabrication of information - protection of information
Personality traits		Intention to adopt new online services / technologies
Web / online / computer skills		
Previous online privacy (negative) experience	**PRICON** **Online privacy concern**	Future online usage
Need for privacy online		Towards collection of personal information
Privacy awareness		
Computer anxiety		Towards control of personal information
Time spent online (actively)		
Perceived benefits		Towards degree of regulatory control
Cultural characteristics (individual values)		Sharing private information online
Social trust		

Variables included in the general model of online privacy concern are largely recognized in the literature. However, for most, there is little or no evidence of their impact and its direction in the model. For others, the evidence is ambiguous. Along with our intuition, we explain all the variables included, their respective scales and previous findings from the literature. First we explain the antecedents i.e. determinants of online privacy concern.

2.2. Determinants of online privacy concern

Determinants of online privacy concern are variables on the left side of our model. They are defined as antecedents to online privacy concern and expected to affect the level of privacy concern, yet in most of the cases the direction and strength of this impact are not clear. Let us illustrate this at the rather simple example of demographic variables. Age is assumed to be positively correlated to the level of privacy concern. Younger generations intuitively know how to use technology, and are described as digital natives, and they are less concerned about privacy when online. However, older people might not be aware of new technologies that enable "big brother" functionalities in our everyday life (like built-in locators in smart phones or tracking Internet browsing at personal computers) and are therefore less concerned about protecting their privacy when online. The relationship between male or female Internet users and their privacy concern is not clearly stated in literature but it doesn't mean the gender differences in Croatia do not exist and that is worth exploring. There are some indications in the past research on higher education being related to higher online privacy concern, as well as the negative relationship between income and privacy concern online. On the other hand, more educated citizens might be aware there is no absolute privacy protection guaranteed; one can't control information flows over the Internet and beyond, and so this part of the population may be more resilient to loosing online privacy. The same stands for profession, since some occupations and jobs performed might affect person's privacy concern. It is reasonable to suppose that an ICT expert is at least more knowledgeable about privacy issues when online, compared to for example a landscape architect. Income stands in most attitudinal studies as a useful explanatory variable, and as a determinant of online privacy concern. One has to ask if wealthier Internet users care less about privacy infringement. We were interested as well in regional differences, so the variable denoting the county of residence of Croatian citizens surveyed is included into the model. The differences between urban and rural Croatia are hard to capture by the location of the respondent because urban and rural areas in the sense of development and infrastructure are not clearly delineated. The settlement size is more indicative and our intuition gave us

mixed signals. In small settlements people might me more active and deliberated of concerns when online because they had little alternatives in social and cultural life. However this might be equally true for respondents living in large cities. Chen, Zhang, and Heath (2001), Zhang, Chen, and Wen (2002), Janda and Fair (2004), Fogel and Nehmad (2009), Hoy and Milne (2010), Ji and Lieber (2010), Joinson et al. (2010) all investigate the relationship between demographic characteristics of the individuals on privacy concern.

Cheng, Zhang, and Heath (2001) do not find the connection between age, income, education and privacy concern, except for the individuals without online shopping experience. For these individuals they find positive correlation between age and concern for unauthorized use of credit cards. Hoy and Milne (2010) find that women are significantly more concerned about their privacy on Facebook. Janda and Fair (2004) confirm this conclusion, as well as Joinson et al. (2010) and Fogel and Nehmad (2009). Hoy and Milne (2010) also find positive connection between age and privacy concern. Ji and Lieber (2010), on the other hand, do not find unambiguous evidence of impact of gender, age or education on privacy concern. Zhang, Chen, and Wen (2002) do not find evidence of impact of education and income on privacy concern in the United States, but ascertain the connection between income, age and privacy concern in China. Age was found to have negative impact on privacy concern in China. To conclude on demographic variables and privacy concern, in this research, the following variables are included: total monthly household income, age, occupation, gender, education, county of residence and settlement size.

Next variable included in the model represents personality traits. Personality must somehow determine our attitudes and behaviour in our everyday life, and online activities certainly make a considerable part of our daily activities. Li (2011) notes that personality traits are underexplored in the online privacy concern literature. Junglas, Johnson, and Spitzmuller (2008) investigate the impact of personality traits on online privacy concern through Big 5 model of personality traits. The five factors have been defined as openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism. They find that agreeableness, conscientiousness, and openness to experience affect online privacy

concern. Korzaan and Boswell (2008) find that agreeableness has significant influence on individual concern for information privacy. The fact that so far, to the best of our knowledge, only two papers address this important issue is enough to motivate us to look further into the potential importance of personality traits for online privacy concern. Therefore we included the shortened version of Big 5 psychological assesments, developed by Rammstedt and John (2007) in the research model. The shortened version of Big 5 is developed and tested by Rammstedt and John, (2007). It includes self-ratings on how person sees him/herself as someone who is reserved, gets nervous easily, is generally trusting, had an active imagination, does a thorough job, is outgoing/sociable, etc. enabling us to describe the personality of individuals in Croatia.

Another underexplored, yet important determinant of online privacy concern is culture. Bellman et al. (2004) investigate the impact of cultural values, regulatory structure and Internet usage experience on privacy concern. They find the effects of three cultural dimensions of online privacy concern: power distance, individualism and uncertainty avoidance. However, the impact is completely mediated by the regulatory structure. Milberg, Smith, and Burke (2000) confirm the effect of culture on privacy concern – power distance, individualism and masculinity have a positive impact on privacy concern and uncertainty avoidance negative. It is widely recognized fact in the literature that there are differences between the cultures with regards to privacy concern (Dinev et al. 2005; Chiou, Chen, and Bisset, 2009; Ur and Wang, 2013). It is therefore crucial to advance the understanding of influence of individual level cultural values on privacy concern.

Internet knowledge and skills should alleviate privacy concerns. The reason is that skilled Internet users are more knowledgeable about the privacy risks and are able to customize Internet browsers and applications in a way to protect their privacy (Dinev and Hart, 2005). The opposite direction of this relationship is possible in the cases of Internet addicted part of population, as some young Internet users might not be concerned about privacy. Intensity of using the Internet for a range of available services might be either positively or negatively related to online privacy concern, and there is a reasonable assumption that the time spent

online actively should influence the respondent's online privacy concern.

Aversion towards computerization might be connected to the increased privacy concern when online. Therefore we have included computer anxiety variable as a determinant in our PRICON model. Factors affecting computer anxiety refer to the extent of fear or aversion to computerization and/or interactions with computers that is manifested in people (Parasuraman and Igbaria, 1990) and previous research found that computer anxiety affects users' performance in software (Thomas, 1994).

Negative previous experience is also expected to determine the level of online privacy concern, and is used by Okazaki, Li, and Hirose (2009), and this should be positively correlated. Actual negative experience of the respondent or somebody close to him/her connected to privacy intrusion, steeling data or Internet fraud should considerably alter privacy concern of the victim or witness of the privacy intrusion act.

Privacy awareness is the consciousness of an individual about the importance of privacy and privacy threats. People might or might not be aware of the fact that everything ever posted on the web remains there forever and might be (mis)used. The privacy awareness is the awareness of privacy policy practices of both government and business sectors. It is closely related to the desire of an individual to control information and to be informed about privacy issues. The privacy awareness might have positive and negative influence on online privacy concern. A person with a better knowledge on the privacy policy put in place might see the leakages in the system and that will increase his or her online privacy concern. On the other hand, if a person feels safe and well informed about the privacy protection, he or she should be less concerned about his/her privacy when online. Need for privacy is posited as having a positive effect on online privacy concern. This is in line with current findings from Yao, Rice, and Wallis (2007) and Xu et al. (2008). Need for privacy is strongly opposed to nothing to hide argument. And finally, social trust is supposed to stand as a key factor in building individual's trust towards institutions and other people. The more trust we have, the less concerned about our online privacy we are.

The importance of trust raises in the Internet transactions because of the increased uncertainty and risks of on-line transactions. Pavlou (2002) integrated trust and perceived risks into the Technology Acceptance Model (TAM) and empirically tested it for application in the e-commerce, which is particularly sensitive to the consumer's trust and level of the risk perceptions. He distinguishes privacy risk in the behavioural uncertainty (opportunity for web sites (retailers) to disclose personal (consumer) information) and in the environmental context because of the probability of illegal disclosure or theft of private information. This antecedent of privacy concern is included in our model as perceived benefits, i.e. the trade off an Internet user makes between giving away his/her privacy in exchange for information or service obtained from the Internet.

2.3. Consequences of privacy concern

Implications of online privacy concern are listed on the right side of our model. These are consequences of online privacy concern divided into two groups: attitudes and behaviour. Attitudes do not necessarily reflect behaviour. The expected consequence of an increased online privacy concern is altered protective behaviour in the form of withholding information, providing false information or protection of information, including technical protection (e.g. software installed). Lwin et al. (2007) stated that reactive behaviour implies personal information fabrication, withholding and protecting by using privacy enhancing technologies.

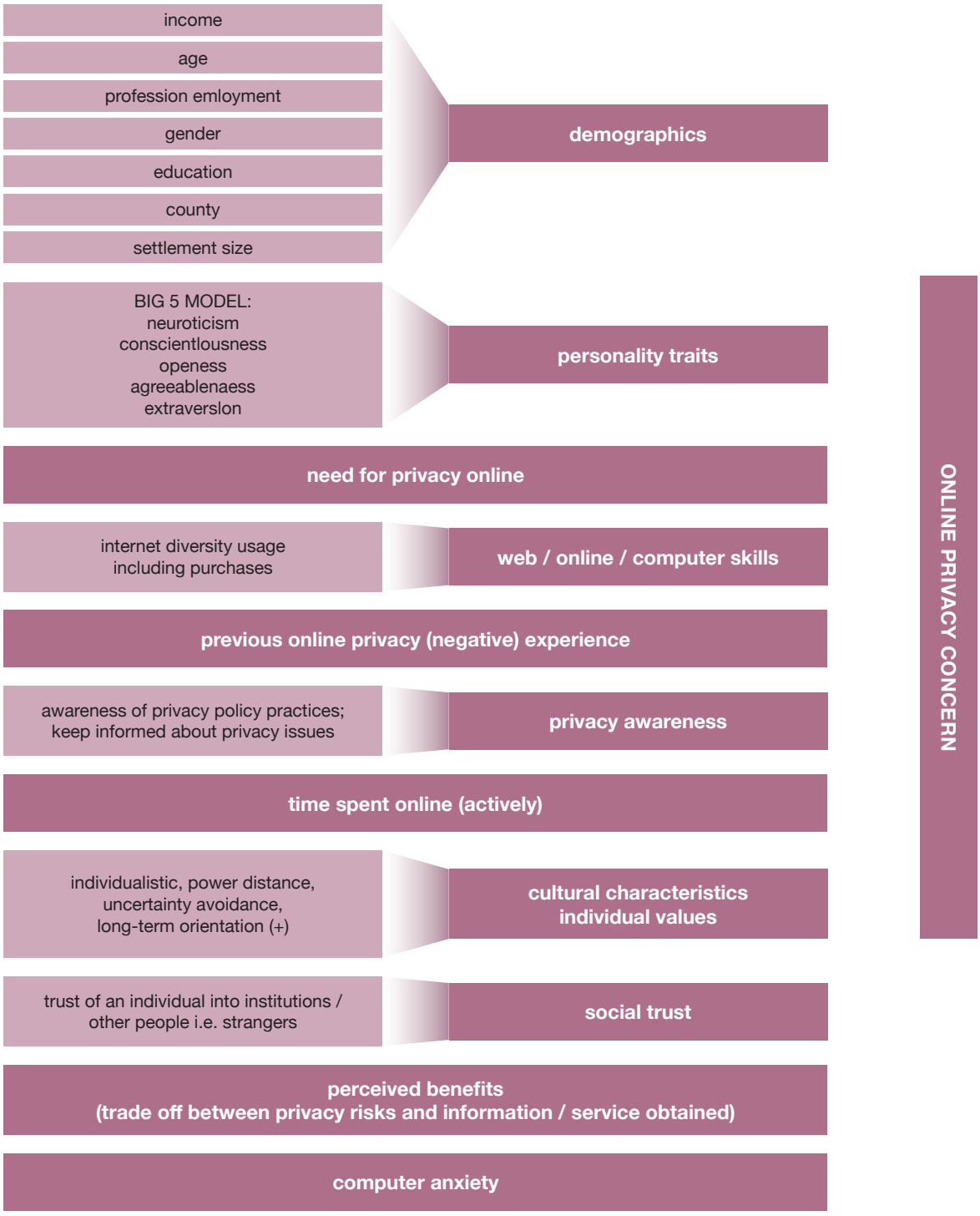
Another behavioural reaction to an increased online privacy concern is less online usage in the future, including refrain from surfing on the Internet or limiting the range of online activities. People concerned about their privacy when online might change their intention to adopt new online services or technologies. More concerned users might decide not to make online purchases, or e-banking transactions. Some concerned people might refrain from social networks or even from using smartphones. Online privacy concern is expected to shape our attitudes towards collection of personal information and towards control of personal information provided (Malhotra, Kim, and Agarwal, 2004). This refers for example to the agencies that collect, analyze and manipulate the personal data collected from their customers. Is it OK for agencies and companies to track online activities of an individual

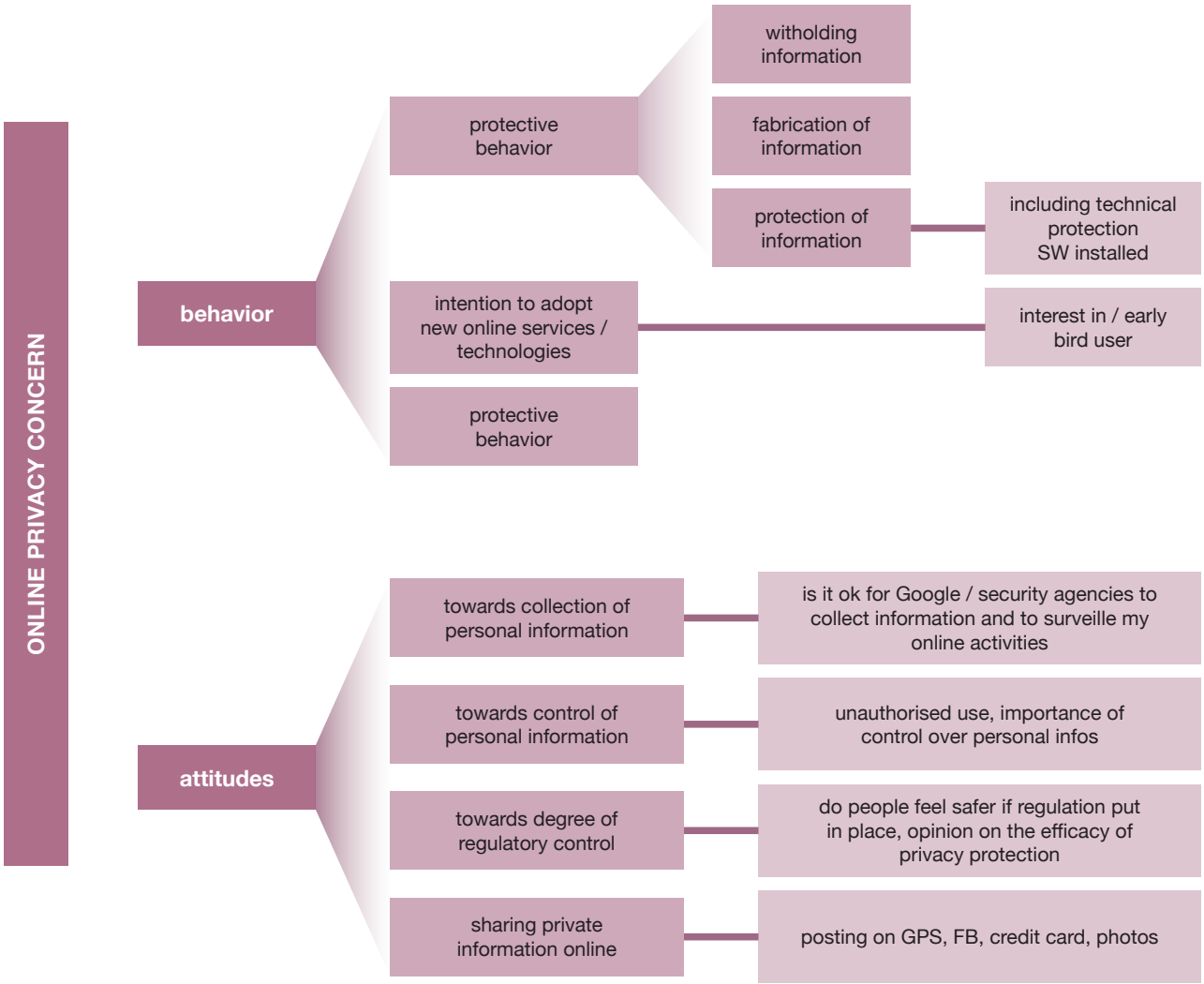
in order to collect data without noticing and getting prior consent of a person? How far should security agencies go in surveilling people and in data mining, and is there an effective regulatory protection? Under the influence of online privacy concern people change attitudes towards a degree of regulatory control and sharing private information online (Lwin, Wirtz, and Williams, 2007; Wirtz, Lwin, and Williams, 2007).

More concerned Internet users would be very cautious to expose themselves more than necessary and avoid activities over the Internet such as posting private data on Facebook, sending personal medical record by email, provide credit card number online, send photos on the Internet, etc. This might be in particular true for mid-aged citizens and the elderly.

All these variables are included in the integrated model of online privacy concern. Finally, the PRICON model we empirically tested is presented in Figure 2.

Figure 2. PRICON model




ONLINE PRIVACY CONCERN
behavior
protective behavior
witholding information
fabrication of information
protection of information
including technical protection SW installed
intention to adopt new online services / technologies
interest in / early bird user
protective behavior
attitudes
towards collection of personal information
is it ok for Google / security agencies to collect information and to surveille my online activities
towards control of personal information
unauthorised use, importance of control over personal infos
towards degree of regulatory control
do people feel safer if regulation put in place, opinion on the efficacy of privacy protection
sharing private information online
posting on GPS, FB, credit card, photos

3. SURVEY DEVELOPMENT

Upon building a model, a customized survey questionnaire was designed and measurement instruments for variables tested. The field research consisted of surveying 2,000 citizens in Croatia – Internet users, to assess their attitudes and behaviour patterns when taking different roles and actions in the online environment. This core part of the research aimed to empirically test the conceptualized model by employing adequate analytical tools to the large database collected in the survey. In this chapter we provide detailed description of all phases of the survey.

3.1. Semi-structured interviews

Before conducting a survey, theoretical model was tested in the preliminary research based on semi-structured interviews. In the next section we describe the methodology applied and the results of this qualitative preliminary research, which served as baseline for the design of the survey. The objectives of this exploratory research could be summarised as follows: (i) to identify and study specific issues of online privacy concern and (ii) to provide inputs for designing questionnaires to be used for survey in the next stage of research.

In this exploratory research, qualitative methodological approach was employed. In particular, semi-structured interviews were conducted in order to explore in more detail experiences when dealing with online privacy concern. All the steps were taken to follow qualitative research methodology described in Berg (1995). Semi – structured interview guide, which can be found in Appendix A, was prepared by Edo Rajh (ER) while the interviews were done by him and other project members: Jelena Budak (JB), Ivan-Damir Anić (IDA), Vedran Recher (VR), Vatroslav Škare (VS) and Bruno Škrinjarić (BS). When selecting candidates for the interview, each project member selected few of its friends and relatives, keeping in mind to differentiate total interview sample to as many different age groups, occupations and education backgrounds. The only pre-requisite for someone to be suitable for the interview was that she or he was an Internet user. All of the interviews were conducted face to face, as this was the best way to get interviewee feedback regarding our topic. These semi-structured

interviews were conducted throughout July, August and September 2015.

During the course of the interview, questions were directed toward exploration of topics related to attitudes on online privacy concern. Each interview was done by one interviewer who asked questions and made notes. All interviews were conducted in Croatian language. Afterwards, interview notes were transcribed and sent to interviewees for verification. Verified notes from interviews were used for writing the cases. Since researcher effects are one of the possible biases in qualitative research (Miles and Huberman, 1994), and the involvement of several researchers in case study development was important to avoid this bias, project members who didn't participate in the interviews were actively involved in writing the cases. In addition, triangulation by researcher (Denzin, 1978), which positively affects research validity, was used.

As already mentioned, data in exploratory research was collected using semi-structured interviews. In total we conducted 15 interviews starting from July 13, 2015 until September 4, 2015. Basic interviewees' data are presented in Table 3. Most of the interviews lasted 15 minutes and 60 percent of our interviewees were women. Age of the interviewees ranged from 23 to 63 years, with the average value of 44.34 years, with men being slightly older than women. In terms of highest obtained education level, seven interviewees finished secondary school (equivalent to ISCED level 3), seven people completed tertiary education (equivalent to ISCED level 5) and one interviewee had a doctoral degree (equivalent to ISCED level 6). Occupations of interviewees varied from being a student, through various other occupations, to being unemployed. We made sure that no two interviewees with same occupation are present. Finally, most of the interviewees resided in Zagreb, but we also covered a part of Dalmatia region (Split) and Slavonija region (Vukovar and Osijek).

Table 3. Basic respondent's data in semi-structured interviews

No	Interviewer	Date	Duration (mins)	Gender	Age	Education	Occupation	Residence
1	BS1	20.07.2015	15	F	23	Secondary	Student	Velika Gorica
2	BS2	25.08.2015	25	F	31	Doctoral	Research associate	Zagreb
3	ER1	29.08.2015	20	M	39	Secondary	Trader	Vukovar
4	ER2	01.09.2015	20	M	40	Tertiary	Medical doctor	Osijek
5	ER3	02.09.2015	8	F	63	Secondary	Dental technician	Vukovar
6	ER4	03.09.2015	15	F	38	Tertiary	Pharmacist	Zagreb
7	IDA1	13.07.2015	20	F	59	Secondary	Senior statistician	Zagreb
8	IDA2	13.07.2015	15	F	52	Secondary	Accounting referee	Zagreb
9	JB1	25.08.2015	15	M	50	Tertiary	Senior consultant	Zagreb
10	JB2	25.08.2015	20	M	50	Secondary	Unemployed	Zagreb
11	JB3	04.09.2015	15	M	45	Secondary	Head of Sales	Zagreb
12	VR1	29.07.2015	20	F	35	Tertiary	Librarian	Zagreb
13	VR2	03.08.2015	10	F	56	Tertiary	Unemployed	Zagreb
14	VS1	24.08.2015	18	F	37	Tertiary	Theological collaborator	Split
15	VS2	25.08.2015	15	M	47	Tertiary	Legal officer	Split

For the purpose of case studies we briefly asked interviewees about their Internet usage, online privacy concerns and any behaviour changes that might have occurred as a result of previous bad experiences. They provided useful insights into online privacy issues that enabled us to better understand antecedents and consequences of online privacy concern. Most of the interviewees use Internet for all kinds of purposes. Everyone stated they

primarily use Internet for e-mail services and browsing for information, both of personal and business nature. Six people listed using Internet banking while eight people reported that they frequently use Internet for online shopping. Other mentioned Internet uses include: downloading and reading online books and articles, using chatting rooms and systems, music and video streaming and downloading, and visiting school and e-diary websites for family members.

When asked how much time daily they spend on the Internet, the most common reply was around 2 hours, though some stated they may go on a few days without going online. Those whose job description is tightly linked to using a computer and Internet spend from 10 to 15 hours online. Most of the younger respondents started using Internet in their youth, while they were in primary or secondary school, while the older respondents started using Internet primarily at the workplace. All of the interviewees were connecting to the Internet using desktop computers and smartphones, while six of them were also using laptops and / or tablet computer. Seven out of fifteen interviewees responded positively when asked whether there are any aspects of the Internet that causes them concern. Three of them stated that the biggest issue was the unprotected use of their personal data (such as name, surname, address, phone number…) and especially of credit card numbers and other financially sensitive data. Other four interviewees had different concerns, namely: exposure of children to contents inappropriate to their age, decreasing quality of online information coupled with numerous annoying advertisements, concern of web-viruses and loss of "human" component in online communication. Eight people responded they don't have any concerns regarding Internet usage. Most of them did not mention why, but amongst those who did, general consensus was that they do not visit suspicious Internet sites, that someone can obtain their information regardless of their Internet usage and that some eager hacker can access your account regardless of online protection you use. Moving on to online privacy concern, five interviewees expressed their concerns, mainly due to the possibility of financial fraud and identity theft. Others weren't concerned about their online privacy. Most of them argued that you yourself chose what you put online and you should be aware of the consequences. Furthermore, they express the opinion that nothing is so important in their lives that they

would need special protection against, or they would need to hide. When asked what they do to protect their online privacy, the most common answer was to provide as few details as possible, inputting only the required information when asked, and often inputting alias e-mail addresses and other information. Some of them frequently use antivirus, malware and firewall software scans, modify the privacy settings on their accounts and use complicated, more difficult to break, usernames and passwords. Six interviewees stated they had adapted their behaviour with regards to their online privacy concern. Two of them mentioned they stopped using social networks (such as Facebook or Instagram), two mentioned they no longer buy online nor use Internet banking, and two of them said they payed greater attention to what sites they were visiting and which information they are inputting. Other nine interviewees declared no change in their online behaviour.

When asked if there are certain activities they no longer wish to do while online, ten interviewees answered positively. Five of them said they had minimised or stopped altogether buying online or any other activities involving their financial information. Four reported they minimised posting their personal pictures or pictures of their family and children on social media, minimised posting delicate updates on their profile on social media or their location on some instant messaging applications (like Viber or WhatsApp). One also expressed caution about uploading his files on online cloud type storage and synchronization services (like Dropbox, Google Drive, One Drive or iCloud). Finally, eight interviewees agreed there was a way of reducing online privacy concern. Three of them mentioned that government should do more to inform citizens about regulations and safety issues whilst online, and also adopt more severe punishments for those who abuse someone's online privacy. Two respondents highlighted the role of "dot.com" enterprises in a way that they should provide possibility of making an online purchase without providing confidential financial information. Another two respondents said it was up to us to be more careful about what we put online, what sites we visit and whether or not we provide sensitive privacy information online. One respondent recognized that she lacked knowledge about online privacy issues at the time and that she would benefit from more education on this topic. Three respondents expressed their doubts about any form of diminishing online privacy risk. They claim there is no bulletproof way of

protecting against the attacks of more and more sophisticated hackers. Four respondents had nothing to say about this.

Semi – structured interviews enabled us to identify certain patterns regarding online privacy concern. Because of the small sample size it is impossible to infer causal relationship between variables, but that was not the intent of this exploratory research. Still, it is quite common to employ qualitative research as the exploratory study in order to design quantitative survey (Silverman, 2006). From methodology perspective, this approach contributes to the quality of survey and methodological rigor.

As expected, half of the respondents are concerned by at least some aspect of Internet use, and one third of respondents stated their concerns about privacy online. Almost all respondents revealed the necessity to include various antecedents and consequences of online privacy concern recognized in the literature in the general model (Dinev and Hart, 2006; Wirtz, Lwin, and Williams, 2007; Xu, Dinev, Smith, and Hart, 2008). For example, almost all respondents listed at least some part of protective behaviour online – whether it was providing minimum information required, fabricating e-mail addresses or using software to protect their privacy. In conversation with the respondents, theoretical model based on literature review was largely confirmed. In line with this, we proceeded with the development of the questionnaire that was used in the survey to gather data for research; aimed at measuring the interrelations between antecedents and consequences of online privacy concern in order to observe the causal relationships in the model.

3.2. Questionnaire design and codebook

The survey questionnaire had to be designed in the way that it should include items that describe all the variables in the PRICON model. Most of items were taken from the literature and in the process of developing the survey instrument, we adapted some of them in order to capture better the model we aimed to empirically test. Some of the items were added as a result of internal PRICON workshops and briefings and brought novelty into the research. The most important advancements from the literature were made in order to build the large

all-encompassing integral model of online privacy concern. Finally, it had to suite the survey sample i.e. Croatian population of Internet users. The introductory note was intended to increase confidence in the survey and in the anonymity of data collected, and consequently to increase the response rate and decrease the drop-out rate. The questionnaire in English is provided in Appendix B with abbreviations corresponding to the codebook used. Items in the English version of the questionnaire are left intentionally grouped by variables in order to make it easy to understand the logic of designing the survey tool. Therefore, the form of the English version of the questionnaire does not correspond to the form of the Croatian version used in the field work (Appendix C).

The first elimination question is if a respondent is a person who is using Internet, and if they were we checked the intensity of using the Internet by an open question measuring hours spent on the Internet per typical day.

Variable representing web and online skills (WEB) is measured by the set of 15 statements examining for what activity a person is using the Internet, e.g. for e-mails, for social network, for online education, Internet shopping, e-banking, for making phone calls, playing online games, or other. The yes or no answers are rather simple for the respondent and put at the very beginning of the questionnaire, followed by the question on the future intensity of online usage (FUT).

The 5 point- Likert scale questions were introduced in the survey instrument at the set of ten statements describing personality traits of a respondent (PT), taken from the Big 5 literature (Rammstedt and John, 2007). Privacy awareness variable (AW) was measured by five scales taken from Xu, Dinev, Smith, and Hart (2008) and Malhotra, Kim, and Agarwal, 2004 (adapted). It focuses on how well a person is informed about privacy issues, if he/she follows the new developments in privacy matters and how interested a person is in privacy protection and related issues in general. For both PT and AW items respondents were asked to express the level of agreement from 1 = Strongly disagree to 5 = Strongly agree. The wordings in Likert scale answers are used from Vagias, (2006). Don't know answers were not provided as an option.

Individual values (V) reflecting cultural set of values a person possesses were measured by a standard Schwartz value survey, SVS (Schwartz, 1992). Originally SVS used 57 value items to represent ten motivationally distinct values that are theoretically derived from universal requirements of human life. These are namely, Power, Achievement, Hedonism, Stimulation, Self-Direction, Universalism, Benevolence, Tradition, Conformity, and Security. Based on the SVS, Lindeman and Verkasalo (2005) developed the shortened Schwartz's value survey consisting of one item for one value. Therefore we used ten measures for individual values asking respondents to what extent the following ideas represent a life-guiding principle for them personally.

To measure social trust (ST), two sets of questions was employed, one for measuring the trust in institutions and another measuring general trust in people (Naef and Schupp, 2009).

Perceived benefits (BNF) of services or information that can be obtained over the Internet were measured using the adapted constructs and scales of Dinev and Hart (2006) and Malhotra, Kim, and Agarwal (2004). Respondents were also asked about trading off the potential privacy violations risks in the sake of personal interest to get information or services online.

Considering the need for privacy when online (NO), three statements were used to explore people's general opinion on preserving anonymity when using the Internet, and about retaining the control and deliberate consent on gathering personal information when online (items were partly used from Yao, Rice, and Wallis, 2007).

Fear of technology and concern about the negative aspects of computerization and frustration related to computer anxiety (CA) were measured using the adapted items of Parasuraman and Igbaria (1990).

The central variable in PRICON model is online privacy concern (OPC). Here we borrowed six constructs from Smith, Milberg, and Burke (1996), covering various aspects of personal online privacy concern. Respondents were asked if they were concerned about their online

privacy on the scale from 1 to 5. Furthermore, we were interested into their views on Internet causing serious privacy problems. Respondents evaluated how sensitive they were about the way of handling personal information online in comparison to other people. Finally, they evaluated how much personally they are concerned about extensive collection of privacy information on the Internet, how important online privacy is for them, compared to other subjects related to Internet usage.

Items exploring attitudes towards collection of personal information (ATT) were adapted from Malhotra, Kim, and Agarwal (2004). A respondent was asked about invasive activities of websites, such as if tracking his/her online activities, asking for personal information or collecting too much personal information bothers him/her a lot. Items related to the control of personal information and unauthorized secondary use (CTRL) actually assess personal opinion on how private information should be handled over the Internet. Understanding what online privacy means to a person in terms of rights and the autonomy to decide how personal information is collected, used, and shared and if control lies in the core of privacy were taken from Malhotra, Kim, and Agarwal (2004). Two other CTRL items were taken from Smith, Milberg, and Burke (1996) and refer to the purpose of allowed usage of collected information, with or without authorization of the person.

The perceived degree of regulatory control (REG) and its efficiency was measured by three items. Respondents were asked to declare if the existing country legislation and government effort was sufficient to protect online privacy (Lwin, Wirtz, and Williams, 2007) or there should be more strict regulation put in place to protect personal privacy online (Wirtz, Lwin, and Williams, 2007).

Willingness to share private information online (SH) was investigated by asking about the different types of information at the different sharing platforms such as social networks. We asked if people put private information on the Internet, share private pictures, post their current location or company, and finally provide the credit card number when buying online.

Protective behaviour (PB) was assessed by a set of ten statements asking for how often a respondent behaved in some of the listed ways when on the Internet (Wirtz, Lwin, and Williams, 2007). The answers were provided on the 5-point scale ranging from never to every time. Some of the examples of behaviour include giving false responses, using another e-mail address to hide the real identity, using the special privacy protection software, refusing to provide personal information to untrustworthy websites or avoid visiting such websites, and finally, avoiding purchasing from untrustworthy websites.

Intent to adopt new technologies (IT) was asked about in form of two separate questions (as used in Wang, Dacko, and Gad, 2008). The first question was if the respondent was a new-technology follower due to His/her interests (not abilities) to use new online services or technologies. The second question asked for the likelihood of being an early user of new online services or technologies as soon as they were available.

Items on previous experience (PE) were put in rather simple yes or no questions. We distinguished if a person or somebody close to him/her had bad experiences with regard to privacy violation on the internet before, or to the previous experience with privacy violation in general (adapted from Li, 2014).

At the end of the questionnaire we inquired about buying online habits asking if a person had ever bought goods or services on the Internet, and if so what was the intensity of online purchasing in last six months.

Finally, demographic characteristics of individual respondents (D) were captured by asking for age in years, education in terms of primary school or less, secondary, tertiary education or master / doctoral degree. The interviewer noted the gender of respondent, and asked for the number of household member. This enabled calculation of an average income per capita, since later the data on total net average monthly income of household was asked. In order to avoid no answer to this delicate question, the offered answers were systemized into seven categories corresponding to the income brackets in Croatia, expressed in local currency kuna.

As online privacy concern might depend on the job performed and employment status, we asked for the occupation of respondent in five categories corresponding to the international classification (owner/craft, self-employed, manager/official, professional, and technician/clerk) and whether he/she is unemployed, student or retired. Here we offered an option of open question to provide “other” answer as well.

Finally, the regional distribution was recorded in the questionnaire by interviewer who knew in advance which county telephone number extension he/she dialled. The respondent had to name his/her settlement and provide details on the settlement size in terms of number of inhabitants (four size brackets were provided).

The total of 19 variables and one elimination question (filter question for our sample consisting of Internet users only) were used in coding the questionnaire (Table 4).

Table 4. Codebook for variables in the PRICON model questionnaire

Code	Variable
F	**F**ilter question
D	**D**emographics
PT	**P**ersonality **T**raits
WEB	**WEB** / online / computer skills
PE	**P**revious **E**xperience
AW	Privacy **AW**areness
T	**T**ime Spent Online Actively
V	Individual **V**alues
ST	**S**ocial **T**rust
NO	**N**eed for **O**nline Privacy
BNF	Perceived **B**e**N**e**F**its
CA	**C**omputer **A**nxiety
OPC	**O**nline **P**rivacy **C**oncern
PB	**P**rotective **B**ehaviour
IT	**I**ntent to Adopt New **T**echnologies
FUT	**FUT**ure online usage
ATT	**ATT**itudes Towards Collection of Personal Information
REG	Degree of **REG**ulatory Control
SH	**SH**aring Private Information Online
CTRL	**C**on**TR**o**L** of Personal Information and Unauthorized Secondary Use

3.3. Survey (sampling, CATI)

Internet users in Croatia represent the population for this study. Secondary data were used (Stilus Media) to assess the number of Internet users in Croatia, and online phone book was used as a sampling frame. The sample was made on a one-way stratification by 21 counties. The sample allocated to each stratum was proportional to the assessed number of Internet users each stratum. Within each stratum, a combination of random and systematic sampling was applied. Pages from phone book were selected using simple random sampling procedure. Sample units within each page were selected applying systematic sampling procedure. The final sample consists of 2060 Internet users aged 18 or older.

A survey was conducted from November 2015 to February 2016, with final stratum completion in March 2016. For the purposes of conducting the survey, 12 interviewers were employed whose sole job was to contact respondents and record their answers. Within the Institute of Economics, Zagreb, each of them was assigned a separate telephone line and a laptop computer with Computer-Assisted Telephone Interviewing (CATI) software installed. To be more precise, we used "Creative Research System" and their 11.0 version of Survey system software. For further inquiries about the mentioned software, examples and help files, the reader is directed to their official website[1].

This mode of recording answers required that all of 19 variables, as presented in Table 4, be coded in Survey system itself. Each question, possible answers, routing and all the explanation marks were entered as in the paper version of questionnaire, presented in Appendix C. During the selection process of interviewers, we made the highest priority that they possess adequate IT skills, and afterwards acquainted them with CATI method of data collection. After every day of data collection process, all the responses were exported as a MS Excel table and stored on an external hard drive as a back-up. Upon the completion of data collection, all the responses were polled in one spreadsheet which we used as primary

1 http://www.surveysystem.com/index.htm

data source. Collected data were checked for internal and logical consistencies to ensure high quality of collected data. Finally, all collected data were prepared for further analysis in Stata, Statistica and R.

4. DESCRIPTIVE STATISTICS

Here we present basic descriptive statistics from our obtained sample. Table 5 presents the descriptive statistics of latent variables (indented are the items of particular variable). The dataset has 2060 observations and variables, and values presented here are measured on Likert scale, ranging from 1 to 5. The only exception is the estimation of daily average of active time spent on the Internet, which is ranging from 0.5 hours to 24 hours. On average, 3.22 hours are spent daily on using the Internet and relatively high standard deviation (2.87) implies large degree of variation among respondents. Following the section with personality traits, the average participant does not consider him/herself to be neurotic and art inclined person, since both mean values are below 3 (2.47 and 2.87 respectively). On the other hand, most of the people consider themselves to be sociable and lazy with tendency to find fault with others. Regarding the personal values, the average person does not consider power, authority and wealth as important as honesty, responsibility, equality, broadmindedness etc. It should be noted that the unusually low mean value of 1.99 for “materialistic” section might be explained by underreporting. Apparent lack of social trust can be observed not only towards individuals, but towards institutions too. On average, people do not consider others to be trustworthy and it is recommended to proceed with caution when dealing with strangers before trusting them. However, more concerning is distrust in public authorities and courts manifested with low means (2.27 and 2.70 respectively). This phenomenon may partially be explained by the perception of high level of corruption in public authorities and judiciary system in Croatia (Transparency International).

Table 5. Descriptive statistics of latent variables

Variable	N	Mean	Std. Dev.	Min	Max
Time	2060	3.22	2.87	0.5	24
Personality traits					
Extraversion	2060	3.92	0.87	1	5
Agreeableness	2060	3.96	0.70	1	5
Conscientiousness	2060	4.09	0.84	1	5
Neuroticism	2060	2.47	0.96	1	5
Openness	2060	2.87	0.86	1	5
I see myself as someone who ...					
... is reserved	2060	3.46	1.33	1	5
... is outgoing, sociable	2060	4.38	0.84	1	5
... is generally trusting	2060	3.58	1.06	1	5
... tends to find fault with others	2060	4.35	0.88	1	5
... tends to be lazy	2060	4.17	1.10	1	5
... does a thorough job	2060	4.01	1.02	1	5
... is relaxed, handles stress well	2060	2.49	1.12	1	5
... gets nervous easily	2060	2.44	1.20	1	5
... has few artistic interests	2060	2.53	1.39	1	5
... has an active imagination	2060	3.20	1.38	1	5
Personal Values					
Power, authority, wealth	2060	1.99	1.12	1	5
Achievement, success, ambition	2060	3.47	1.19	1	5
Hedonism, gratification of desires	2060	3.72	1.10	1	5
Stimulation, exciting and challenging life	2060	3.36	1.27	1	5
Creativity, freedom, curiosity, independence	2060	4.22	0.94	1	5
Broadmindedness, equality, environment	2060	4.40	0.85	1	5
Benevolence, honesty, responsibility	2060	4.65	0.59	1	5
Tradition, humbleness, modesty	2060	4.02	1.05	1	5
Obedience, honouring elders, politeness	2060	4.50	0.73	1	5
Security, social order, cleanliness	2060	4.30	0.90	1	5

Variable	N	Mean	Std. Dev.	Min	Max
Social Trust 1	2060	2.61	0.78	1	5
In strangers you meet first time	2060	2.20	1.06	1	5
In public authorities	2060	2.27	1.10	1	5
In police	2060	3.27	1.15	1	5
In courts	2060	2.70	1.22	1	5
Social Trust 2	2060	3.60	0.66	1	5
In general, I can trust people.	2060	2.75	1.15	1	5
When dealing with strangers, it's better to be cautious before trusting them.	2060	4.45	0.84	1	5
Privacy Awareness	2060	3.92	0.64	1.4	5
I am aware of the privacy issues and practices in our society.	2060	4.08	0.95	1	5
I follow the news and developments about the privacy issues and privacy violations.	2060	3.55	1.14	1	5
I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy.	2060	2.98	1.20	1	5
Web sites seeking information online should disclose the way the data are collected, processed and used.	2060	4.42	0.81	1	5
A good online privacy policy should have a clear and conspicuous disclosure.	2060	4.55	0.73	1	5
Personal Internet Benefits	2060	2.92	1.16	1	5
In general, my need to obtain certain information or services from the Internet is greater than my concern about privacy.	2060	3.05	1.32	1	5
I find that personal interest in the information that I want to obtain from the Internet overrides my concerns of possible risk or vulnerability that I may have regarding my privacy.	2060	2.91	1.30	1	5
The greater my interest to obtain a certain information or service from the Internet, the more I tend to suppress my privacy concerns.	2060	2.81	1.28	1	5
Online Privacy Need	2060	4.27	0.65	1	5
People should be able to use the Internet anonymously.	2060	3.61	1.33	1	5
People have the right to control personal information about them when online.	2060	4.58	0.67	1	5
There should be no personal information gathering on the internet without consent.	2060	4.60	0.73	1	5
Computer Anxiety	2060	2.94	1.06	1	5
Computers are a real threat to privacy in this country.	2060	3.54	1.32	1	5

Variable	N	Mean	Std. Dev.	Min	Max
I am anxious and concerned about the pace of automation in the world.	2060	3.02	1.40	1	5
I am easily frustrated by increased computerization in my life.	2060	2.25	1.24	1	5
Online Privacy Concern	2060	3.56	0.96	1	5
I am concerned about my online privacy.	2060	3.48	1.31	1	5
All things considered, the Internet would cause serious privacy problems.	2060	3.94	1.08	1	5
Compared to others, I am more sensitive about the way my personal information is handled online.	2060	3.18	1.31	1	5
I am concerned about extensive collection of my personal information over the Internet.	2060	3.36	1.39	1	5
I am concerned about my privacy violation when using the internet.	2060	3.34	1.35	1	5
Compared with other subjects on my mind, personal privacy online is very important.	2060	4.05	1.04	1	5
Attitudes Towards Collection of Personal Info	2060	2.78	0.79	1	5
It doesn't bother me when websites track my online activities.	2060	2.42	1.44	1	5
It doesn't bother me when websites ask me for personal information.	2060	2.31	1.37	1	5
I'm concerned that websites are collecting too much personal information about me.	2060	3.60	1.39	1	5
Control of Personal Information Online	2060	4.56	0.57	1	5
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.	2060	4.47	0.76	1	5
My control of personal information lies at the heart of my privacy.	2060	4.42	0.82	1	5
Personal information should not be used for any purpose unless it has been authorized by that person.	2060	4.67	0.64	1	5
When people give personal information for some reason, it should never be used for any other reason.	2060	4.68	0.65	1	5
Degree of Regulatory Control	2060	3.06	0.60	1	5
The existing laws in my country are sufficient to protect people online privacy.	2060	2.59	1.01	1	5
The government is doing enough to ensure that citizens are protected against online privacy violations.	2060	2.44	1.00	1	5

Variable	N	Mean	Std. Dev.	Min	Max
There should be tougher regulations by the government to protect personal privacy online.	2060	4.15	0.93	1	5
Sharing Private Information Online	2060	2.12	0.95	1	5
I don't mind sharing private pictures on the Internet.	2060	2.42	1.33	1	5
I put private information on the Internet.	2060	2.01	1.18	1	5
I don't mind posting on the Internet information about the place I am at the moment.	2060	1.95	1.20	1	5
I don't mind posting on the Internet with who I am at the moment.	2060	1.97	1.21	1	5
I see no problem in sending my credit card data when buying online.	2060	2.25	1.36	1	5
Protective Behaviour	2060	2.98	0.57	1	5
I give fictitious responses to avoid giving the web site real information about myself.	2060	1.88	1.15	1	5
I use another name or e-mail address when registering with certain web site without divulging my real identity.	2060	1.78	1.16	1	5
When registering with certain web site, I only fill up data partially.	2060	2.63	1.48	1	5
I use software so that the recipient cannot track the origin of my mail.	2060	1.76	1.26	1	5
I use software to eliminate cookies that track my Internet activities.	2060	2.06	1.48	1	5
I use software to disguise my identity.	2060	1.60	1.10	1	5
I am reluctant to register with my personal information to the websites I don't completely trust.	2060	4.37	1.02	1	5
I refuse to provide personal information to untrustworthy websites.	2060	4.58	0.80	1	5
I avoid visiting the untrustworthy websites.	2060	4.52	0.81	1	5
I don't purchase goods from untrustworthy websites.	2060	4.59	0.86	1	5
How interested would you be in using new online services /technologies immediately after they're available?	2060	3.08	1.05	1	5
What is the likelihood that you will be one of the early users of new online services / technologies immediately after they are available?	2060	2.28	1.08	1	5
How many times in last six months have you bought goods or services on the Internet?	1389	0.18	0.38	0	500
People living in your household	2060	0.14	0.34	1	12

Regarding the privacy awareness, the average citizen is aware of the privacy issues and practices in the society. Furthermore, he/she considers that web sites seeking information should be transparent over data collection and usage. Also, the news and developments about the privacy issues and privacy violations are followed (mean 3.55), but the solutions presented by the companies and government aimed at privacy issues are not well communicated (mean 2.98).

Average citizen does not consider the benefits of gathering information being greater than his/her concern for privacy. The need for online privacy is well manifested, since the prevailing opinion is that an individual should be able to control personal information when online and that gathering information should not be conducted without the individual's consent. Also, there is a relatively negative attitude towards collection of personal information and a strong consent over ability to control personal information online.

Average citizen considers the current degree of regulatory control of personal information online insufficient. Interestingly, mean value of tendency to share private information online is 2.12 which can be translated as disapproval with that notion, with highest animosity towards sharing location and the name of the partner. Protective behaviour during online sessions is limited in avoiding or submitting personal information to untrustworthy websites, while no protective software or other method is used for "trustworthy" websites.

Finally, interesting responses were given by 1389 citizens when asked for the number of purchases online of goods and services in the last month. Mean value of 0.18 implies very low online purchase culture in Croatia.

Descriptive statistics of dummy variables is presented in Table 6. In the first section, the respondents were asked about the web usage items. The most frequent item is General information with 97.77% frequency, followed by E-mails and Daily news, which scored 94.17% and 92.86%, respectively.

Table 6. Descriptive statistics of dummy variables

Variable	N	Freq.	Freq. (%)
Web usage items			
E-mails	2060	1940	94.17%
IM services	2060	1232	59.81%
Music/Movie download	2060	917	44.51%
Online games	2060	592	28.74%
Internet banking	2060	1236	60.00%
Online education	2060	330	16.02%
Online shopping	2060	1251	60.73%
Radio streaming	2060	892	43.30%
Watching videos	2060	1791	86.94%
Online calls	2060	1563	75.87%
Social networks	2060	1519	73.74%
Daily news	2060	1913	92.86%
General information	2060	2014	97.77%
Online forums	2060	645	31.31%
Public services	2060	800	38.83%
Future Internet Usage Intentions			
Less	2060	79	3.83%
About the same	2060	1538	74.66%
More	2060	443	21.50%
Have you or somebody close to you have had bad experiences with regard to privacy violation on the internet before?	2060	364	17.67%
Have you or somebody close to you have had bad experiences with regard to privacy violation in general?	2060	280	13.59%
Have you ever bought goods or services on the Internet?	2060	1393	67.62%

On the other hand, Online education is the most sporadic item with only 330 out of 2060 respondents reporting its usage. Similarly, future internet usage is intended by 74.66% individuals, while only 3.83% intend to use it less. Privacy violation on the internet (17.67%) is slightly more reported than the privacy violation in general (13.59%). Finally, 67.62% individuals had experience with purchasing goods or services on the internet.

Descriptive statistics of demographic variables is shown in Table 7. According to different socio-economic criteria, the whole sample of 2060 individuals has been divided in subgroups. Regarding the education groups, the most common education attainment level is secondary education with 50.24% frequency. By narrow margin (50.29% vs. 49.71%), female respondents are more numerous than their male counterparts. Participants aged between 18 and 29 form relative majority of the sample (27.23%). Among occupation groups, the most reported occupation is professional (29.90%), followed by worker (24.66%). With respect to income groups, 29.17% of participants in the sample receive income in the range of 7.501- 10.000 HRK, which is higher than the average salary of 5.704 HRK in 2015 (Croatian National Bank). According to official territorial classification, the sample has been divided in 21 units, namely 20 counties and the City of Zagreb. Relative majority of participants reported its residence in the City of Zagreb (18.98%) which is followed by the Split-Dalmatia county (10.34%) and the Zagreb county (7.43%). At last, size of the settlement was taken as criterion for differentiating subgroups in the sample. In big cities (the ones with more than 100.000 inhabitants) lives 35.87% of the respondents, while 35.49% has their residence in small cities (from 10.001 inhabitants to 50.000 inhabitants).

Table 7. Descriptive statistics of demographic variables

Variable	N	Freq.	Freq. (%)
Education groups			
primary school or less	2060	17	0.83%
secondary education	2060	1035	50.24%
tertiary educ./high school, university	2060	945	45.87%
master degree/doctoral title	2060	63	3.06%
Gender			
Female	2060	1036	50.29%
Male	2060	1024	49.71%
Age groups			
18 - 29	2060	561	27.23%
30 - 39	2060	552	26.80%
40 - 49	2060	470	22.82%
50 - 59	2060	346	16.80%
60+	2060	131	6.36%
Occupation groups			
Owner of the company / craft	2060	42	2.04%
Manager/official	2060	44	2.14%
Professional	2060	616	29.90%
Technician/clerk	2060	373	18.11%
Worker	2060	508	24.66%
Retired	2060	180	8.74%
Student	2060	180	8.74%
Unemployed	2060	103	5.00%
Other	2060	14	0.68%
Income groups			
up to 2.500 HRK	2060	51	2.48%
2.501-5.000 HRK	2060	305	14.81%
5.001-7.500 HRK	2060	451	21.89%

Variable	N	Freq.	Freq. (%)
7.501-10.000 HRK	2060	601	29.17%
10.001-12.500 HRK	2060	274	13.30%
12.501-15.000 HRK	2060	197	9.56%
more than 15.000 HRK	2060	181	8.79%
County			
Zagreb	2060	153	7.43%
Krapina-Zagorje	2060	63	3.06%
Sisak-Moslavina	2060	88	4.27%
Karlovac	2060	61	2.96%
Varaždin	2060	82	3.98%
Korpivnica-Križevci	2060	55	2.67%
Bjalovar-Bilogora	2060	58	2.82%
Primorje-Gorski Kotar	2060	141	6.84%
Lika-Senj	2060	24	1.17%
Virovitica-Podravina	2060	44	2.14%
Požega-Slavonia	2060	41	1.99%
Brod-Posavina	2060	75	3.64%
Zadar	2060	80	3.88%
Osijek-Baranja	2060	143	6.94%
Šibenik-Knin	2060	56	2.72%
Vukovar-Srijem	2060	84	4.08%
Split-Dalmatia	2060	213	10.34%
Istarska	2060	97	4.71%
Dubrovnik-Neretva	2060	57	2.77%
Međimurje	2060	54	2.62%
City of Zagreb	2060	391	18.98%
Size of the settlement groups			
10.000 or less	2060	279	13.54%
10.001-50.000	2060	731	35.49%
50.001-100.000	2060	311	15.10%
more than 100.000	2060	739	35.87%

Descriptive statistics of latent variables in cases when using gender as a differentiation criterion is presented in Table 8. In the personality traits section, women characterize themselves as being more extroverted, agreeable and conscientious. Men consider themselves to be less neurotic than women do and openness is reported more among male participants. Even though there are no radical differences in personal values between men and women, as means are relatively close to each other, certain conclusions can be drawn. In average, men are more prone to a hedonistic style of life. The biggest difference between men and women can be observed in the level of dismissal of power, authority, and wealth as personality characteristics. Mean value for men is 2.09, while for women is 1.90. Also, women emphasize the importance of honesty, equality, politeness, politeness and other features more.

Social distrust is present among both men and women, with women having relatively more confidence in public institutions (2.63 compared with 2.59 for men). General distrust towards people and caution prior to trusting strangers is on the same level for men and women with mean value 3.6. Privacy awareness, computer anxiety, online privacy concern and control of personal information online are more dominant among female population, while personal internet benefits, attitudes, sharing private information online and protective behaviour is more characteristic for men.

Table 8. Descriptive statistics of latent variables by gender

Latent variable / Gender		Male				Female				
Time	N	Mean	Std. Dev.	Min	Max	N	Mean	Std. Dev.	Min	Max
Personality traits										
Extraversion	1024	3.86	0.86	1.5	5	1036	3.98	0.87	1	5
Agreeableness	1024	3.93	0.69	1	5	1036	4.00	0.70	1	5
Conscientiousness	1024	3.98	0.87	1	5	1036	4.20	0.80	1	5
Neuroticism	1024	2.40	0.96	1	5	1036	2.53	0.95	1	5
Openness	1024	2.96	0.86	1	5	1036	2.78	0.85	1	5
Personal Values										
Power, authority, wealth	1024	2.09	1.15	1	5	1036	1.90	1.08	1	5
Achievement, success, ambition	1024	3.49	1.15	1	5	1036	3.45	1.23	1	5
Hedonism, gratification of desires	1024	3.73	1.08	1	5	1036	3.70	1.12	1	5
Stimulation, exciting and challenging life	1024	3.42	1.24	1	5	1036	3.30	1.31	1	5
Creativity, freedom, curiosity, independence	1024	4.20	0.96	1	5	1036	4.25	0.92	1	5
Broadmindedness, equality, environment	1024	4.32	0.89	1	5	1036	4.49	0.81	1	5
Benevolence, honesty, responsibility	1024	4.57	0.65	1	5	1036	4.72	0.52	1	5
Tradition, humbleness, modesty	1024	3.96	1.04	1	5	1036	4.08	1.06	1	5
Obedience, honouring elders, politeness	1024	4.45	0.76	1	5	1036	4.56	0.70	1	5
Security, social order, cleanliness	1024	4.26	0.91	1	5	1036	4.34	0.88	1	5
Social Trust 1	1024	2.59	0.80	1	5	1036	2.63	0.75	1	5
Social Trust 2	1024	3.60	0.67	1	5	1036	3.60	0.64	1	5
Privacy Awareness	1024	3.89	0.64	1.6	5	1036	3.95	0.63	1.4	5
Personal Internet Benefits	1024	2.99	1.12	1	5	1036	2.86	1.20	1	5
Online Privacy Need	1024	4.27	0.67	1	5	1036	4.27	0.64	1.7	5
Computer Anxiety	1024	2.83	1.06	1	5	1036	3.04	1.05	1	5
Online Privacy Concern	1024	3.50	0.96	1	5	1036	3.62	0.95	1	5
Attitudes Towards Collection of Personal Info	1024	2.80	0.79	1	5	1036	2.76	0.80	1	5
Control of Personal Info Online	1024	4.50	0.62	1	5	1036	4.62	0.52	2	5
Degree of Regulatory Control	1024	3.06	0.62	1	5	1036	3.06	0.58	1	5
Sharing Private Information Online	1024	2.22	0.95	1	5	1036	2.02	0.94	1	5
Protective Behaviour	1024	2.99	0.61	1	5	1036	2.97	0.54	1	5

Table 9. Descriptive statistics of latent variables by age groups

Latent variable / Age groups	18 - 29			30 - 39			40 - 49			50 - 59			60 +		
Time	N	Mean	Std. Dev.	N	Mean	Std. Dev.	N	Mean	Std. Dev.	N	Mean	Std. Dev.	N	Mean	Std. Dev.
Personality traits															
Extraversion	561	3.86	0.83	552	3.92	0.88	470	3.93	0.88	346	3.97	0.87	131	4.00	0.87
Agreeableness	561	3.91	0.70	552	3.94	0.68	470	3.97	0.71	346	4.04	0.67	131	4.05	0.70
Conscientiousness	561	3.85	0.88	552	4.13	0.79	470	4.22	0.80	346	4.21	0.82	131	4.22	0.85
Neuroticism	561	2.43	0.91	552	2.47	0.93	470	2.53	1.03	346	2.48	0.97	131	2.31	0.99
Openness	561	3.11	0.81	552	2.84	0.84	470	2.80	0.88	346	2.74	0.86	131	2.54	0.82
Personal Values															
Power, authority, wealth	561	2.30	1.16	552	1.94	1.08	470	1.78	1.08	346	1.89	1.04	131	1.94	1.22
Achievement, success, ambition	561	3.85	0.97	552	3.49	1.20	470	3.24	1.24	346	3.23	1.25	131	3.23	1.25
Hedonism, gratification of desires	561	4.04	0.96	552	3.76	1.07	470	3.62	1.13	346	3.43	1.13	131	3.21	1.23
Stimulation, exciting and challenging life	561	3.79	1.08	552	3.46	1.23	470	3.26	1.27	346	2.98	1.32	131	2.44	1.31
Creativity, freedom, curiosity, independence	561	4.28	0.84	552	4.18	0.99	470	4.30	0.88	346	4.12	1.05	131	4.18	0.94
Broadmindedness, equality, environment	561	4.23	0.92	552	4.38	0.86	470	4.52	0.78	346	4.52	0.77	131	4.52	0.84
Benevolence, honesty, responsibility	561	4.53	0.65	552	4.63	0.59	470	4.70	0.57	346	4.76	0.48	131	4.73	0.61
Tradition, humbleness, modesty	561	3.75	1.13	552	4.05	0.98	470	4.06	1.05	346	4.21	0.99	131	4.34	0.92
Obedience, honouring elders, politeness	561	4.33	0.82	552	4.49	0.74	470	4.58	0.66	346	4.62	0.64	131	4.69	0.60
Security, social order, cleanliness	561	4.07	0.99	552	4.28	0.92	470	4.40	0.82	346	4.50	0.78	131	4.41	0.77
Social Trust 1	561	2.64	0.75	552	2.64	0.75	470	2.67	0.80	346	2.48	0.82	131	2.50	0.81
Social Trust 2	561	3.52	0.67	552	3.56	0.63	470	3.61	0.60	346	3.73	0.69	131	3.77	0.78

Latent variable / Age groups	18 - 29			30 - 39			40 - 49			50 - 59			60 +		
Time	N	Mean	Std. Dev.	N	Mean	Std. Dev.	N	Mean	Std. Dev.	N	Mean	Std. Dev.	N	Mean	Std. Dev.
Privacy Awareness	561	3.86	0.60	552	3.88	0.66	470	3.95	0.64	346	4.00	0.62	131	3.98	0.69
Personal Internet Benefits	561	3.18	1.06	552	2.92	1.12	470	2.83	1.20	346	2.70	1.25	131	2.71	1.21
Online Privacy Need	561	4.31	0.66	552	4.25	0.66	470	4.29	0.64	346	4.24	0.65	131	4.16	0.68
Computer Anxiety	561	2.79	1.00	552	2.98	1.05	470	2.94	1.08	346	3.03	1.10	131	3.09	1.11
Online Privacy Concern	561	3.46	0.93	552	3.56	0.98	470	3.60	0.94	346	3.66	0.97	131	3.56	1.01
Attitudes Towards Collection of Personal Info	561	2.80	0.79	552	2.74	0.74	470	2.80	0.80	346	2.74	0.83	131	2.83	0.85
Control of Personal Info Online	561	4.41	0.62	552	4.57	0.55	470	4.60	0.58	346	4.69	0.49	131	4.65	0.53
Degree of Regulatory Control	561	3.03	0.60	552	3.06	0.57	470	3.07	0.58	346	3.05	0.64	131	3.18	0.71
Sharing Private Information Online	561	2.65	0.90	552	2.11	0.91	470	1.93	0.91	346	1.74	0.79	131	1.57	0.80
Protective Behaviour	561	3.14	0.63	552	3.01	0.53	470	2.92	0.52	346	2.84	0.52	131	2.77	0.63

Table 10. Descriptive statistics of latent variables by education level

Latent variable / Education group	Primary or less			Secondary			Tertiary			PhD or Postgrad		
	N	Mean	Std. Dev.	N	Mean	Std. Dev.	N	Mean	Std. Dev.	N	Mean	Std. Dev.
Personality traits												
Extraversion	17	4.15	0.52	1035	3.96	0.86	945	3.88	0.88	63	3.87	0.81
Agreeableness	17	3.97	0.54	1035	3.96	0.71	945	3.97	0.68	63	4.04	0.75
Conscientiousness	17	4.32	0.66	1035	4.07	0.89	945	4.11	0.79	63	4.17	0.75
Neuroticism	17	2.03	0.67	1035	2.40	0.95	945	2.54	0.95	63	2.60	1.15
Openness	17	2.53	0.84	1035	2.92	0.89	945	2.82	0.84	63	2.87	0.70
Personal Values												
Power, authority, wealth	17	2.29	1.31	1035	1.98	1.16	945	2.00	1.08	63	2.02	1.07
Achievement, success, ambition	17	2.82	1.29	1035	3.48	1.22	945	3.48	1.16	63	3.43	1.10
Hedonism, gratification of desires	17	3.06	0.97	1035	3.74	1.10	945	3.72	1.10	63	3.54	1.16
Stimulation, exciting and challenging life	17	2.35	1.00	1035	3.27	1.32	945	3.44	1.23	63	3.79	0.99
Creativity, freedom, curiosity, independence	17	3.24	1.30	1035	4.16	1.00	945	4.29	0.86	63	4.43	0.76
Broadmindedness, equality, environment	17	4.59	0.62	1035	4.45	0.84	945	4.36	0.88	63	4.40	0.77
Benevolence, honesty, responsibility	17	4.59	0.51	1035	4.68	0.55	945	4.61	0.63	63	4.62	0.55
Tradition, humbleness, modesty	17	4.47	0.80	1035	4.19	0.95	945	3.86	1.10	63	3.40	1.24
Obedience, honouring elders, politeness	17	4.65	0.61	1035	4.60	0.66	945	4.42	0.77	63	4.14	0.95
Security, social order, cleanliness	17	4.59	0.62	1035	4.46	0.80	945	4.15	0.94	63	3.73	1.17
Social Trust 1	17	2.53	0.72	1035	2.58	0.77	945	2.64	0.78	63	2.69	0.88
Social Trust 2	17	3.59	0.59	1035	3.57	0.67	945	3.63	0.65	63	3.59	0.56
Privacy Awareness	17	3.56	0.40	1035	3.99	0.65	945	3.85	0.61	63	3.77	0.68
Personal Internet Benefits	17	2.53	1.23	1035	2.81	1.19	945	3.02	1.13	63	3.32	0.99
Online Privacy Need	17	4.33	0.41	1035	4.29	0.66	945	4.25	0.65	63	4.18	0.74
Computer Anxiety	17	3.33	0.92	1035	3.01	1.08	945	2.87	1.04	63	2.58	0.95
Online Privacy Concern	17	4.08	0.82	1035	3.64	0.97	945	3.47	0.93	63	3.45	0.97
Attitudes Towards Collection of Personal Info	17	2.57	0.65	1035	2.82	0.84	945	2.74	0.73	63	2.79	0.91
Control of Personal Info Online	17	4.54	0.57	1035	4.61	0.55	945	4.52	0.58	63	4.28	0.68
Degree of Regulatory Control	17	3.27	0.63	1035	3.06	0.62	945	3.08	0.59	63	2.89	0.60
Sharing Private Information Online	17	1.72	0.78	1035	2.07	0.95	945	2.17	0.94	63	2.34	1.00
Protective Behaviour	17	2.79	0.71	1035	2.99	0.59	945	2.97	0.55	63	3.03	0.54

Table 9 shows inter-generational differences in attitudes and opinions. Extraversion and agreeableness is gradually more reported as the group is older. On the other hand, openness, which is characterized as active imagination and art preference, is more dominant among youngest population with consequent decline towards the eldest population. Neuroticism appears in inverse U shape, as it is most reported among people aged 40 to 49. Conscientiousness is on its lowest among youngest people and grows until the age of 40, when it stabilizes. Youngest population describes themselves relatively more driven by wealth, power, ambition and hedonistic style than the rest of the population, with "materialistic" and hedonistic factors gradually declining with aging. On the other hand, "conservative" values, such as obedience, tradition and politeness become more characteristic as a person gets older.

Trust in public institutions is low among all age groups, but it is relatively the lowest among people aged 50 or more. On the other hand, general trust in people and caution towards strangers grows with age. Personal internet benefits are more emphasized among youngest population, while computer anxiety is reported highest in the eldest population. Also, sharing private information online and protective behaviour are prevalent among people aged 18-29.

In Table 10 we can see descriptive statistics by education level. Extraversion gradually decreases with education level, while neuroticism shows opposite trend. Hedonism and challenging life are most dominant for people with secondary and tertiary education, while power, authority and wealth score most among least educated people. Also, creativity and freedom rise with education attainment which can't be said for the subgroup of "conservative" values, such as obedience, tradition and security, which decrease with more years of education. General trust in people is relatively equal among all education levels but the trust in public institutions grows with years of schooling.

While the attitudes and opinions of people with secondary and tertiary education are similar throughout the questionnaire, the biggest difference regarding the answers of various education groups can be observed between two extremes – primary education and PhD level.

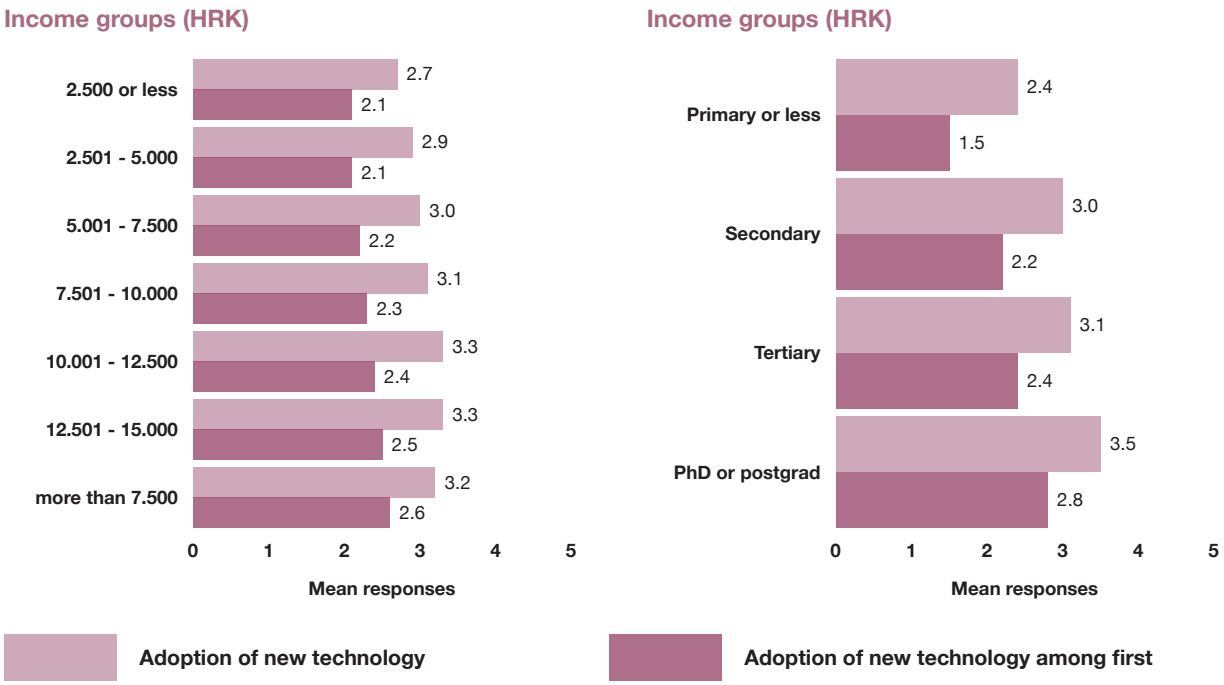
Online privacy need and concern, computer anxiety and demanded degree of regulatory control are more attributed to the primary education attainment and gradually decrease with further education. In contrast, protective behaviour, recognition of personal internet benefits and sharing private information online is more outlined among more educated groups.

Figure 3 further expands this analysis by comparing different aspects of online behaviour by education. Online privacy concern diminishes with the level of education, as well as a desired degree of regulatory control. Hence, individuals with primary education are more concerned about privacy than more educated respondents. Also, control of personal information online is relatively more reported among respondents with lower levels of education. Finally, sharing private information online is a matter of concern among all categories. However, discontent gradually decreases with years of schooling.

Figure 3. Different aspects of online behaviour by education

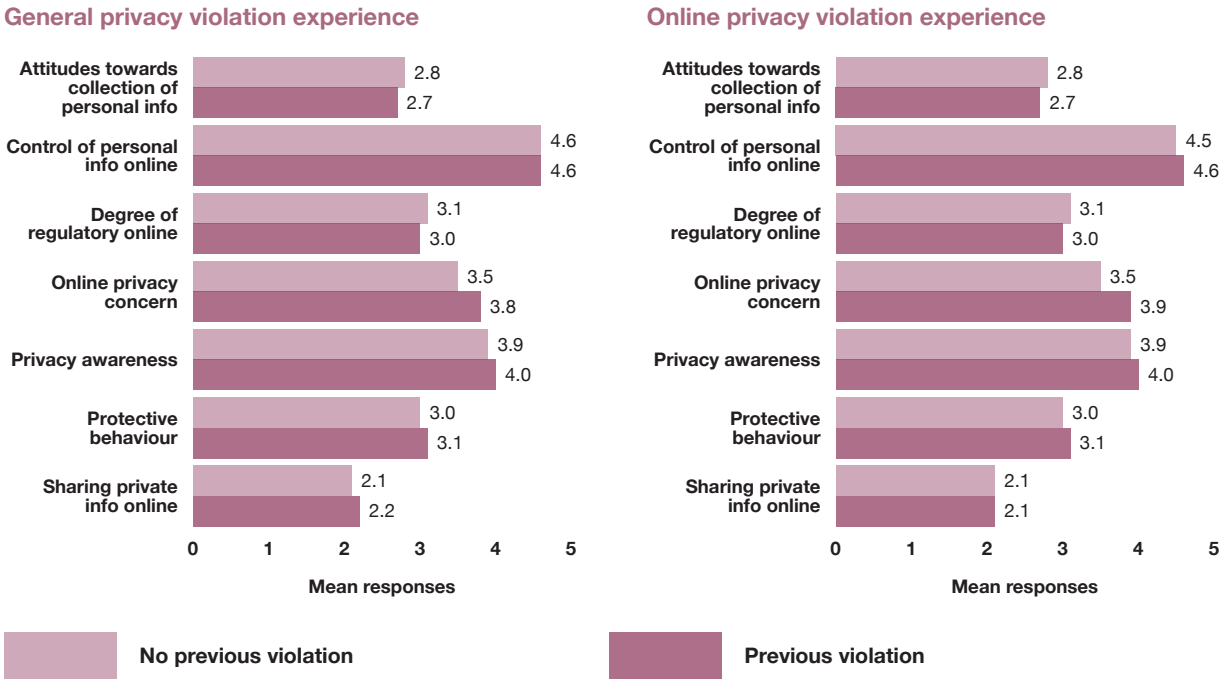
Figure 4 shows interest in new online services and technologies (Adoption of new technology) and probability of purchasing them shortly after market breakthrough (Adoption of new technology among first) by education and income. Values on vertical axis represent different income and education groups. Similar pattern can be observed in both groups. Higher income and education groups gradually increase interest and probability of purchasing new technologies and services. For instance, respondents with PhD degree are almost two times (2.8 vs. 1.5) more likely to buy new technologies and services than the respondents with primary level of education.

Figure 4. New technology use by income and education



In Figure 5, the difference in online behaviour between respondents who experienced privacy breach and those who did not is presented. Surprisingly, attitudes and opinions appear similar. The only significant difference can be observed in Online privacy concern, where expectedly people whose privacy (in general and online) had been violated in the past show more concern than the others. However, anticipated difference in other variables, such as Protective behaviour and Sharing private info online, is negligible.

Figure 5. Online behaviour by previous privacy violation experience



Based on the preliminary analysis, and before testing the entire model, we proceeded with the deeper analysis of the parts of the model. At the antecedents' side, we examined the relation among personal values and beliefs of Internet users in Croatia, the effect of personality traits and regulatory factors to privacy concern. The following chapters present empirical analyses as they have been produced for research papers. Some of them have been printed ad working papers or submitted for publishing. For the sake of safeguarding the parts of the research as a whole, some information in these chapters are being repeated.

5. EMPIRICAL ANALYSIS OF ANTECEDENTS: INTERNET USERS VALUES AND BELIEVES[2]

Culture explains much of the human behavior and social and economic processes in transforming societies (Zmerli and Hooghe (Eds), 2013; Boettke and Coyne, 2009). In post-transition countries this heritage or path dependency (North, 2000) might be even more important. Values are multifaceted constructs that guide thought and action of individuals and have received significant scholarly attention from various academic disciplines. In literature, values are employed to explain and characterize individuals, groups, and societies, as well as to explain and characterize motivational bases behind various attitudes and behavior.

Therefore, we were intrigued to find out whether, and how well, a set of values of an individual in a post-transition country explains his/her actions, attitudes and behavior. Everyday life in the digital environment shifted our focus to Internet users, who make up about two thirds of the adult population in Croatia. Croatia is in terms of the Digital Economy and Society Index (DESI) considered to be a catching-up country when compared to the European Union (EU) average. Regarding the propensity of individuals to use Internet services, Croatia in 2016 scored 0.39 and ranked 23rd in the EU because the percentage of regular Internet users in Croatia was 66 percent, while the EU average was 76 percent (DESI, 2015)[3].

We applied the Schwartz value theory to the survey database of 2,060 Internet users to offer some plausible answers to our research questions: What personal values do Internet users prefer and which ones do they have in common? Could people using the Internet be clustered on the basis of their values, and if so, what explains the differences among groups? Is it all about trust in institutions or in other people as well? Internet users sharing similar values might have similar computer skills or technological anxiety. On the other hand, they might share the same need for privacy and privacy concerns when online. Finally, demographic characteristics such as gender, age, education, income, and occupation usually stand as

2 This chapter was published in September 2016 as Budak, Rajh, and Žokalj: Personal values of Internet users: a cluster analytic approach EIZ-WP-1606 http://www.eizg.hr/hr-HR/Radni-materijali-EIZ-a-207.aspx

3 DESI scores range from 0 to 1; the higher the score, the better the country performance.

explanatory variables in attitudinal studies.

According to our best knowledge, this is the only research on the value sets of individuals that applies the Short Schwartz's Value Survey (SSVS) to a large sample of Internet users in a post-transition country.

5.1. Literature review on social values

The body of literature investigating the impact of personal values, aggregated in culture, uses Hofstede's (1980) dimensions of national culture. The model of national culture in its initial version consists of four dimensions – Power Distance Index (PDI), Individualism vs. Collectivism (IDV), Masculinity vs. Femininity (MAS) and Uncertainty Avoidance Index (UAI).

Power distance shows the degree to which less powerful members of the society accept and expect unequal distribution of power. In societies with a relatively high score, such as Malaysia and the Slovak Republic, the members accept hierarchical distribution of power as a given and do not strive to equalize it among all members of the society.

Individualism indicates the extent to which people's self-image is in terms of "I" rather than "we". Higher values are attributed to societies where it is expected for an individual to take care solely of himself and his closest family (e.g. the United States and Australia), while in collectivist cultures a broader group of individuals is inter-connected in exchange for unquestioning loyalty (e.g. Ecuador and Venezuela).

The masculinity dimension represents societal preference towards material rewards, achievement, heroism and assertiveness or tendency to cooperate, with an emphasis on the care for the weakest members of the society and quality of life in general. Societies with higher score in this dimension (e.g. the Slovak Republic and Japan) are characterized as "tougher" with respect to "tender" cultures (e.g. Sweden and Norway).

The uncertainty avoidance dimension expresses the degree to which the members of a society

deal with the fact that the future can never be known. As a response, countries exhibiting strong UAI (e.g. Portugal, Greece and Uruguay) tend to preserve conservative and traditional codes of behavior and exhibit intolerance towards unorthodox ideas. In Hofstede's later work, the fifth dimension of national culture was added. Long-term orientation (LTO) stands for the fostering of virtues for future rewards, in particular, perseverance and thrift. It is believed that LTO prevails in Asian societies, and that Western-type societies are more short-term oriented in relation to the past and present (Hofstede, Hofstede, and Minkov, 2010).

The relationship between culture and privacy concern is a rather new and underexplored area, and it has been in the center of our particular research interest (Budak, Rajh, Recher, 2016; Recher, Budak, and Rajh, 2016). It is a widely recognized fact in the literature that there are differences between the cultures with regards to privacy concern (Dinev et al. 2005; Chiou, Chen, and Bisset, 2009; Ur and Wang, 2013) and here we build on the previous studies on privacy concern and Hofstede's cultural dimensions.

Milberg, Smith, and Burke (2000) argue that cultural values are strongly correlated with privacy concerns of the population. Power distance, individualism and masculinity are positively connected with privacy concern, while uncertainty avoidance shows negative relationship. Bellman et al. (2004) confirm a statistically significant connection between cultural values and privacy concern. However, they identify influence of cultural values only in two dimensions of information privacy concerns, rather than in overall concern for information privacy, and the impact is completely mediated by the regulatory structure. Furthermore, three dimensions of culture (power distance, individualism and masculinity) had opposite direction of impact on privacy concern with respect to the results in Milberg, Smith, and Burke (2000), while uncertainty avoidance was not significant. In their study, Brashear, Milne, and Kashyap (2006) estimate regression models using primary survey data collected from 18-30 year old users from Brazil, Romania and China. Among Hofstede's four cultural indices, they include uncertainty avoidance and collectivism. Results indicate positive correlation between the degree of uncertainty avoidance and collectivism, and information privacy concern. In China, collectivism is the strongest predictor of privacy concern, while uncertainty avoidance is

the most significant determinant of privacy concern in Romania and Brazil. Cullen (2009) examines privacy concern on the sample of citizens in Japan and New Zealand, with the latter including ethnic minorities (Polynesian natives) to account for different cultural background. The data are obtained through interviews in focus groups. Her results validate the hypothesis that hierarchical-collectivistic cultures, characterized by high power distance attributes within the collectivistic culture, display higher degree of mistrust and privacy concern. Lili and Min (2014) report that power distance, individualism, uncertainty avoidance, and long-term orientation are positively related to privacy concern, while masculinity is negatively related to privacy concern. Furthermore, individualism and uncertainty avoidance significantly affect privacy concern in both Korea and China, with individualism having stronger effect in South Korea than in China. Also, long-term orientation has a significant effect only in Korea, while power distance is significant only in China.

Privacy concern in general differs from privacy concern when online (see more in Gellman and Dixon, 2011). In the last decade, online privacy became the hot topic of information privacy studies. Cho, Rivera, and Lim (2009) surveyed 1,261 Internet users from five cities – Bangalore, Singapore, Seoul, New York and Sydney. Due to the higher relevance in explaining online privacy concern, as well as multicollinearity among indices, only IDV and UAI were employed in the research. Their findings corroborate evidence of a positive relationship between degree of individualism and online privacy concern. However, negative correlation between UAI and privacy concern is in contrast with previous research; thus, the initial hypothesis is only partially supported. Reay et al. (2013) analyze adoption of Platform for Privacy Preferences (P3P) in a sample of 100,000 websites. In line with previous literature, adoption of P3P varies across cultures. Higher individualism is positively connected with P3P adoption, while the correlation is negative for the power distance measure. A statistically significant connection was not identified for the indices measuring masculinity and uncertainty avoidance. Cecere, Le Guel, and Soulie (2015) investigate individuals' Internet privacy concerns with respect to social networking sites on a sample of 22,253 individuals in 26 EU countries. Individualism is negatively related with privacy concerns, which goes in line with findings in Bellman et al. (2004). On the other hand, countries with high levels of masculinity (e.g. Italy and the Slovak

Republic), power distance (e.g. Bulgaria and Romania) and uncertainty avoidance (e.g. Spain, Portugal and Romania) report relatively higher levels of privacy concern. For PDI and UAI, findings confirm the results of Milberg, Smith, and Burke (2000). Miltgen and Peyrat-Guillard (2014) conducted qualitative research on 14 focus groups from 7 EU member states with different socio-economic characteristics. Their research confirms differences regarding online privacy concern with respect to cultural values.

As regards post-transition countries, research on interrelations between cultural characteristics or values and privacy – in particular online privacy concern – is even rarer. In their forthcoming work, Budak, Rajh, and Recher (2016) argue that cultural characteristics of a society determine the level of privacy concerns. They employ data for Croatia from two surveys to explore how Hofstede's indices relate to the privacy concern of Croatian citizens and conclude that data on the individual level might explain interrelations between national cultural dimensions and the level of online privacy concerns better than Hofstede's indices.

Despite being the dominant framework in investigating the connection of cultural values and privacy concern, Hofstede's dimensions of national culture have not escaped criticism. Some researchers argue that they are outdated in the world of rapid changes and globalization. Others reproach over-simplification of culture by reducing it to few dimensions. In line with this argument, Ess and Sudweeks (2005) claim that "having only five or six dimensions for the analysis of culture seems like attempting brain surgery with a bulldozer". Dorfman and Howell (1988) stress the problem of cultural homogeneity, since Hofstede assesses the individual and applies the findings to the overall community. A comprehensive review of criticism of Hofstede's classification can be found in Shaiq et al. (2011). In order to introduce novelty in the research of cultural values and online privacy concern, as well as to overcome the shortcomings of Hofstede's approach, we employed Schwartz's Value Survey (Schwartz, 1992). A thorough presentation of the SVS framework is the topic of the next section.

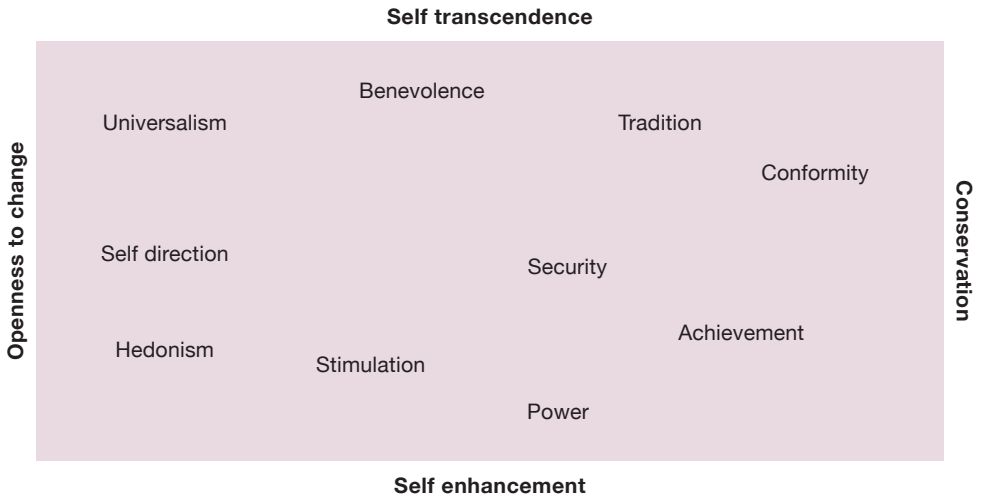
5.2. Schwartz's Value Survey and model applied

According to Schwartz's value theory (Schwartz, 1992; 2012), there are ten motivationally distinct values driven by universal requirements of human life. These values are, namely, power, achievement, hedonism, stimulation, self-direction, universalism, benevolence, tradition, conformity, and security. By asking respondents to what extent the listed ideas represent a life-guiding principle for them personally, 57 value items of Schwartz's Value Survey enable the positioning of an individual in a cultural group. Furthermore, the values form a quasi- circular structure because of the different spacing they occupy, as well as the relations among them. Values close to each other are compatible, while diametrically opposite values are unrelated and incompatible.

Also, the quasi-circular structure indicates existence of two-dimensional space, where the dimensions represent basic human problems. On the one hand, there is a trade-off between conservation and openness to change. Higher motivation for conservation indicates preference towards maintaining current norms and behavior, while motivation to pursue one's own emotional and intellectual interests is the feature of the openness to change dimension. The second dimension is self-transcendence versus self-enhancement, which concerns the conflict between pursuing the welfare of other people and the individual's personal interests.

Lindeman and Verkasalo (2005) developed a shorter version of the original SVS called the Short Schwartz's Value Survey by attributing 10 value items to 10 values, unlike in Schwarz's original survey where 57 value items were corresponding to 10 values. For example, the respondents were asked to grade the importance of "power, that is, social power, authority, wealth" as a life-guiding principle. Their answers were measured on a Likert scale ranging from 0 (opposed to my principles) to 8 (of supreme importance). In their series of studies, they confirmed the validity and reliability of the new scale as well as the quasi-circular structure of the original theoretical framework.

Figure 6. The two-dimensional structure of values



Source: Lindeman and Verkasalo (2005).

Figure 6 is a graphical depiction of the two-dimensional structure of values. On the far ends of the horizontal axis are two opposite motivations – openness to change and conservation, while the vertical axis separates the inclination between self-transcendence and self-enhancement. Depending on the weight that the individual attributes to a specific value item, he/she can be positioned in a broader group of individuals with similar motivation and cultural values.

The Short Schwartz's Value Survey has been widely used in different scientific fields, such as environmental economics (Poortinga et al., 2011), medicine (Saher and Lindeman, 2005), theology (Aarnio and Lindeman, 2015), sociology (Gaunt, 2006), and others. However, to the best of the authors' knowledge, this is the first attempt of examining the correlation between privacy concern and personal values using the SVSS methodology.

We were interested in exploring whether there were differences in these values among groups of citizens in Croatia, and if so, what explained the differences between clusters.

We assume that socio-demographic characteristics of respondents play the major role here. It seems rational that younger people and/or more educated ones are more driven by wealth, power, ambition and hedonistic style than the rest of the population, with gradual decline with years of age. On the other hand, older people have a relatively higher tendency towards "conservative" values, such as obedience, tradition and politeness. Regarding education attainment level, hedonism and challenging life are the most dominant for people with secondary and tertiary education, while self-enhancement and conservation, with their respective values, gradually decline with years of education. The difference between men and women, and the values they assess as life-guiding, is almost negligible. However, men are more prone to a hedonistic style of life, while women attribute more importance to honesty, equality and politeness.

Within the same demographic group, respondents might share various personal values. We posit that for personal values in post-transition countries, the level of trust in institutions and in other people might be crucial. Social trust is a composite variable indicating the degree of confidence towards strangers and institutions. In order to measure it, two sets of questions were employed: one designed to estimate the extent of confidence in institutions and another measuring general trust in people (Naef and Schupp, 2009).

For Internet users surveyed, common personal values might be attributed to the similar computer anxiety and need for privacy online standing as a good proxy for privacy concern shared within the group. In our model, therefore, we include survey questions assessing these attitudes as well. Factors affecting computer anxiety refer to the extent of fear or aversion to computerization and/or interactions with computers that is manifested in people (Parasuraman and Igbaria, 1990) and previous research has found that computer anxiety affects users' performance with software (Thomas, 1994). Computer anxiety, in terms of an unpleasant sense, aversion or fear of using computer technology, or frustration about the computerization going on in the digital society, is measured using the adapted items of Parasuraman and Igbaria (1990).

Need for privacy is strongly opposed with the “nothing to hide” argument. As regards the need for privacy when online, three statements were used to explore people’s general opinion on preserving anonymity when using the Internet, and about retaining the control and deliberate consent on gathering personal information when online (Yao, Rice and Wallis, 2007).

5.3. Data and methodology

The survey data employed originate from the large survey we conducted in Croatia at the beginning of 2016. Data were collected by telephone survey. An online phone book was used as a sampling frame. The sample was created based on a one-way stratification by 21 counties. The sample allocated to each stratum was proportional to the assessed number of Internet users in each stratum. Within each stratum a 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 systematic sampling procedure. The final sample consists of 2,060 Internet users aged 18 or older. The summary statistics of sampled respondents is presented in Table 11.

Table 11. Summary statistics of sampled reposndents, n=2,060

	%
Gender	
Male	49.7
Female	50.3
Age	
18-29	27.2
30-39	26.8
40-49	22.8
50-59	16.8
60+	6.4
Education	
Primary school	0.8
Secondary school	50.2
University and higher education	45.9
Master's degree/doctoral title	3.1
Income	
Up to 2,500 HRK	2.5
2,501-5,000 HRK	14.8
5,001-7,500 HRK	21.9
7,501-10,000 HRK	29.2
10,001-12,500 HRK	13.3
12,501-15,000 HRK	9.6
More than 15,000 HRK	8.8
Occupation	
Owner of the company/craft	2.0
Manager/official	2.1
Professional	29.9
Technician/clerk	18.1
Worker	24.7
Retired	8.7
Student	8.7
Unemployed	5.0
Other	0.7

The measurement instrument included ten questions on values, and ten questions on social trust, need for privacy online and computer anxiety. Each item in the questionnaire was measured by a five-point scale, ranging from 1 (strongly disagree, absolutely no) to 5 (strongly agree, absolutely yes). The demographic variables included gender, age, education, household income, and occupation (see Appendix: Questionnaire).

The collected data were first analyzed in a descriptive manner to determine the public opinion on values, trust and privacy when online. Cronbach's alpha coefficients were calculated to quantify the scale reliabilities. For the second step, exploratory factor analysis was used to identify the factors of personal sets of values. Then, K-means cluster analysis was employed to determine the segments of population with similar values, while differences in respondents' values between the groups were analyzed using chi-square test.

5.4. Results and discussion

The first step in the analysis was the assessment of construct validity and reliability of scales. The initial measurement instrument with 18 items was tested by using exploratory factor analysis. Principal components analysis was employed to extract the factors. The Kaiser-Guttman rule was used to determine the number of factors to extract. After excluding 8 items with loadings greater than 0.5 on more than one factor and items with loadings lower than 0.5 on their primary factor, the exploratory factor analysis indicated four distinct factors, explaining 68.4 percent of the total variance. The factor loadings were greater than 0.50, which is considered sufficient (Bagozzi and Yi, 1988).

Table 12. Exploratory factor analysis results, factor loadings

Items	Factor 1: social trust in institutions	Factor 2: computer anxiety	Factor 3: need for privacy online	Factor 4: social trust in strangers
P3.1				0.82
P3.2	0.74			
P3.3	0.84			
P3.4	0.85			
P4.1				0.78
P4.2			0.85	
P4.3			0.86	
P4.4		0.86		
P4.5		0.75		
P4.6		0.78		

Factors were labelled according to the dominant variables in the factor as follows: factor 1 (P3.2, P3.3, P3.4): social trust in institutions; factor 2 (P4.4, P4.5, P4.6): computer anxiety; factor 3 (P4.2, P4.3): need for privacy online; factor 4 (P3.1, P4.1): social trust in strangers (Table 12).

Confirmatory factor analysis (CFA) was performed to test the convergent and discriminant validity of measures and to detect the unidimensionality of each construct. Unidimensionality is evidence that a single trait or construct underlies a set of measures (Gerbing and Anderson, 1988). The specified measurement model included six uncorrelated factors with uncorrelated measurement errors. The goodness-of-fit index (GFI) and adjusted goodness-of-fit index (AGFI) were 0.98 and 0.95, respectively. The normed fit index (NFI), non-normed fit index (NNFI), comparative fit index (CFI), and RMSEA were 0.94, 0.91, 0.95, and 0.061, respectively. Although the chi-square test was significant, it is important to note that it is sensitive to the sample size. Other model fit indices indicate a reasonable level of fit of the model (Hu and Bentler, 1999). The values of fit indices obtained from the four-factor model represent a

substantial improvement over the values obtained from the one-factor model. The results of confirmatory factor analysis indicate an acceptable level of convergent and discriminant validity, and unidimensionality (Table 13).

Table 13. Confirmatory factor analysis results and Cronbach's alpha coefficients (α)

Items	Factor loadings
Social trust – strangers; α = 0.53	
P3.1	0.52*
P4.1	0.85*
Social trust – institutions; α = 0.75	
P3.2	0.70*
P3.3	0.85*
P3.4	0.92*
Need for privacy online; α = 0.63	
P4.2	0.49*
P4.3	0.47*
Computer anxiety; α = 0.72	
P4.4	0.81*
P4.5	1.21*
P4.6	0.73*

Notes: CFA fit indices: GFI = 0.98; AGFI = 0.95; NFI = 0.94; NNFI = 0.91; CFI = 0.95; RMSEA = 0.061. * Factor loadings significant at $p < 0.01$ level. K-means cluster analysis was employed to classify Internet users in Croatia according to their personal values. The Hartigan index was used as a criterion for determining the number of clusters in a data set. Mean values were calculated for each factor using only the items that remained after the reliability and construct validity assessment. These mean values were taken as an input in the K-means cluster analysis. The K-means cluster analysis indicated three homogeneous segments of citizens (Table 14).

Table 14. Results of K-means cluster analysis, mean values

Values	Sample total (n = 2060)	Cluster 1: power - oriented group (n = 701)	Cluster 2: self - centered group (n = 749)	Cluster 3: self - transcendent group (n = 610)	ANOVA
P2.1 Power	1.99	2.45	2.09	1.35	F = 189.35; p = 0.000
P2.2 Achievement	3.47	3.48	4.02	2.78	F = 219.65; p = 0.000
P2.3 Hedonism	3.72	3.74	4.29	2.99	F = 302.91; p = 0.000
P2.4 Stimulation	3.36	3.62	4.21	2.01	F = 1073.57; p = 0.000
P2.5 Self-direction	4.22	3.99	4.70	3.91	F = 175.24; p = 0.000
P2.6 Universalism	4.40	3.85	4.78	4.58	F = 307.93; p = 0.000
P2.7 Benevolence	4.65	4.19	4.90	4.85	F = 445.77; p = 0.000
P2.8 Tradition	4.02	3.14	4.41	4.54	F = 579.06; p = 0.000
P2.9 Conformity	4.50	3.85	4.85	4.82	F = 705.03; p = 0.000
P2.10 Security	4.30	3.57	4.70	4.64	F = 534.67; p = 0.000
Note: Items were measured on a scale ranging from 1 (absolutely no) to 5 (absolutely yes).					

Source: Survey and authors' calculations.

The average mean values for the total sample show that Croatian Internet users have very little esteem for social power (mean = 1.99) and prefer to reach their life goals by being independent, creative, curious, that is, self-directed. Croats strongly believe in the benevolence of being helpful, honest, responsible and loyal. They respect tradition, self-discipline, security and conformity (all mean values above 4).

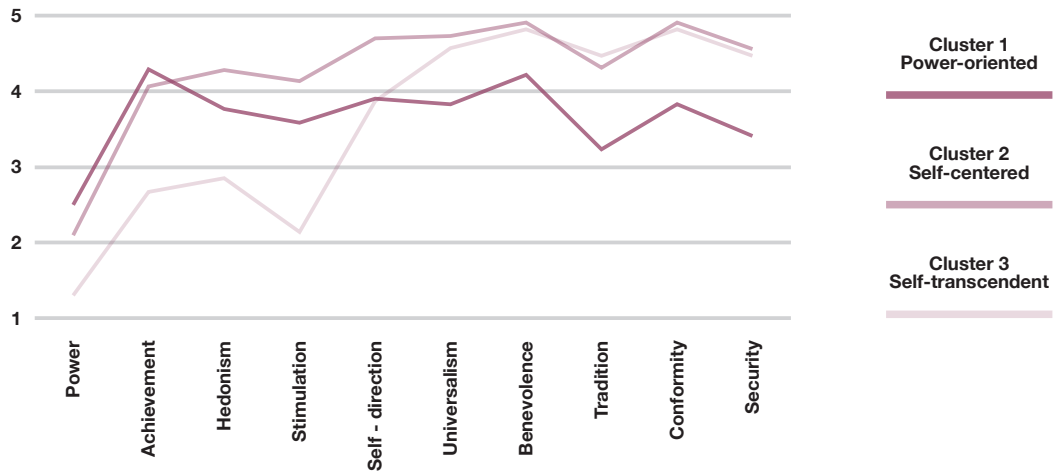
However, three groups of people with different values have been identified as distinguished clusters. Cluster 1 as a power-oriented group has the highest aspiration for achievements, wealth, authority and social power over other people. They do not care much about tradition and may not be described as valuing humbleness, modesty and devotion that go hand in hand with accepting one's role in life. This group has, in comparison with the other two clusters, the lowest mean value of universalism, benevolence, conformity and security. Members of cluster 1 do not value as much the virtues of helpfulness, forgiveness, showing

respect for elderly people, obedience, social justice, equality. Nature, arts, environmental protection and other universalistic concepts do not stand as life-guiding principles for them.

Cluster 2 is a self-centered group because its members are driven by achievement, hedonism, stimulation and self-direction more than people in the other groups (see Figure 7) They, however, share the similar high level of universalism as members of cluster 3, i.e., the self-transcendent group. This means people of both clusters 2 and 3 are driven by universal values in terms of beauty of nature and arts, environment, wisdom and social justice, as well as world peace and equality. Clusters 2 and 3 have similar appreciation for the values of benevolence, conformity and security, but differ significantly in, for example, stimulation that is not a life-guiding principle for the members of self-transcendent cluster 3, while the self-centered members of cluster 2 appreciate the idea of an exciting life very much.

Cluster 3 is a self-transcendent group whose values are tradition, conformity, benevolence and security, contrasted to low stimulation and hedonism values. Members of this cluster do not strive for power and achievements (Figure 7).

Figure 7. Personal-value clusters of Internet users in Croatia



In the core of this research lies the explanation of the differences among clusters. In looking for the attributes of the different value groups of Internet users in Croatia, we first analyzed the demographic characteristics of clusters (Table 15).

In power-oriented cluster 1 there is, as expected, a slight prevalence of male respondents (56 percent of cluster 1 members), while female respondents make up 57 percent of self-transcendent cluster 3. Older people also tend to share the same values of cluster 3, while younger people are more prone to be power-oriented members of cluster 1. Besides these stereotypes, other demographic characteristics are not so evident.

Power-oriented cluster 1 is composed of more educated people (almost 60 percent have university degree or higher), earning an above-average household income (10,000 kuna and more). Striving for success and power is a driving value for company owners, managers, and professionals as well as for students.

Table 15. Differences in demographics among clusters, chi-square test results

		Sample total (n = 2060)	Cluster 1: power-oriented (n = 701)	Cluster 2: self-centered (n = 749)	Cluster 3: self-transcendent (n = 610)	Chi-square test
		1.99	2.45	2.09	1.35	F = 189.35; p = 0.000
Gender	%					
Male		49.7	55.8	46.4	43.1	Pearson chi-square: 20.97; p=0.000
Female		50.3	44.2	50.6	56.9	
Age						
18-29		27.2	36.8	31.2	11.3	Pearson chi-square: 161.71; p=0.000
30-39		26.8	27.3	27.2	25.7	
40-49		22.8	19.3	22.6	27.2	
50-59		16.8	13.0	14.6	23.9	
60+		6.4	3.7	4.4	11.8	
Education	%					
Primary school		0.8	0.7	0.1	1.8	Pearson chi-square: 68.55; p=0.000
Secondary school		50.2	39.9	53.3	58.4	
University and higher education		45.9	54.4	44.5	37.9	
Master's degree/ doctoral title		3.1	5.0	2.1	2.0	
Income	%					
Up to 2,500 HRK		2.5	2.6	1.3	3.8	Pearson chi-square: 105.74; p=0.000
2,501-5,000 HRK		14.8	9.3	14.4	21.6	
5,001-7,500 HRK		21.9	20.1	23.6	21.8	
7,501-10,000 HRK		29.2	26.3	30.7	30.7	
10,001-12,500 HRK		13.3	15.8	13.2	10.5	
12,501-15,000 HRK		9.6	11.1	9.9	7.4	
More than 15,000 HRK		8.8	14.8	6.8	4.3	
Occupation	%					
Owner of the company/craft		2.0	3.7	1.9	0.3	Pearson chi-square: 172.30; p=0.000
Manager/official		2.1	3.9	1.3	1.2	
Professional		29.9	31.4	32.6	24.9	
Technician/clerk		18.1	17.3	18.7	18.4	
Worker		24.7	20.4	24.8	29.3	
Retired		8.7	4.7	6.4	16.2	
Student		8.7	14.3	9.1	2.0	
Unemployed		5.0	3.7	4.7	6.9	
Other		0.7	0.7	0.5	0.8	

Self-centered cluster 2 is a kind of moderate value cluster, with slightly prevalent female members. It attracts Internet population in Croatia aged less than 40 years who in 53 percent of cases have secondary education. The distribution of income subgroups within cluster 2 corresponds perfectly to the average income groups in the whole sample. The largest portion of surveyed professionals and technicians belong to cluster 2.

When it comes to the distinctive characteristics of cluster 3, middle-aged and elderly people are above national average members of self-transcendent cluster 3, as well as Internet users with primary and secondary education and lower household incomes. Workers, as well as unemployed and retired people are predominantly members of this particular cluster.

Next we proceed with the differences in attitudes observed among clusters (Table 16). Power-oriented cluster 1 has the lowest recorded social trust in institutions, opposed to the highest social trust in strangers. They do not care much about privacy, as expressed in no need for privacy online and lack of computer anxiety. Self-centered cluster 2 leads in the level of social trust in institutions and seems to be concerned about privacy online given the highest mean value of need for privacy online score. They demonstrate nearly the average computer anxiety. Self-transcendent members of cluster 3, in line with their demographic characteristics, are predominantly reserved towards strangers and more trustful towards judiciary, political and other institutions. When compared to other groups of Internet users, they express the highest computer anxiety and technology aversion.

Table 16. Differences in attitudes among clusters, ANOVA results

Values	Sample total (n = 2060)	Cluster 1: (n = 701)	Cluster 2: (n = 749)	Cluster 3: (n = 610)	ANOVA
Social trust – strangers	2.48	2.60	2.47	2.34	F = 12.94; p = 0.000
Social trust – institutions	2.75	2.65	2.82	2.77	F = 5.77; p = 0.003
Need for privacy online	4.59	4.41	4.71	4.65	F = 51.14; p = 0.000
Computer anxiety	2.94	2.82	2.95	3.06	F = 8.65; p = 0.000

5.5. Conclusion

This study explores differences in individuals' set of values among Internet users in Croatia. In our first research (Budak, Rajh, and Recher, 2016) we employed Hofstede's scores and observed that cultural dimensions explain privacy concern of the Croatian general population. In this research we employ Schwartz's Value Survey which is more appropriate for individuals, and focus our research on Internet users. Our results, in line with the previous ones (Budak, Rajh, and Recher, 2016), show that online privacy concerns, measured by the expressed need for privacy when online and by computer anxiety, are related to the set of values of groups of Internet users in Croatia. Trust in institutions and in other people explains the differences between clusters as well. Among demographic characteristics, the most pronounced differences between clusters are found in Internet users' age, level of education and income, which is connected with respondents' employment status and occupation. This study, however, does not provide findings on the direction and strength of causal relations. If, for example, older Internet users share more traditional values, does it make them more anxious about computerization, or concerned about privacy protection? Do individual values, demographic characteristics and social trust stand as antecedents of privacy concerns of Internet users in Croatia? All these interesting questions remain to be further explored in an extended model of online privacy concern.

6. THE EFFECT OF PERSONALITY TRAITS ON ONLINE PRIVACY CONCERN[4]

The interaction of online privacy concern and personality traits as one of its antecedents has been the subject of scientific research since relatively recently. With the development of information science and the Internet, online privacy issues have raised the attention of both scholars (e.g. Gellman and Dixon, 2011) and policy-makers (e.g. Henderson, 2015). In addition, there are numerous business areas that might be interested in online privacy concern as well, such as e-commerce and location-based services. The results of the European Commission's survey on "ICT Usage and e-Commerce" (2016) show there is an increase in e-commerce trading. In 2015, 20 percent of enterprises in the European Union (EU) recorded e-sales, which accounted for 16 percent of the total turnover of enterprises. Compared to 2008, the figures increased by 7 and 4 percentage points, respectively. Globally, it is expected that in 2020 e-sales will reach USD 4.1 trillion, with their share in total retail sales doubling compared to the 2015 level (eMarketer, 2016). Another common theme of investigating online privacy concern is the issue of location-based services (Hin et al., 2015). The bulk of mobile phone applications and especially social media contain features which enable data to be collected on the users' whereabouts through GPS tracking. Without discussing the ethical implications, many individuals find the disclosure of their location intrusive or at least express their concerns over potential misuse. Viseu et al. (2004) argued that online privacy issue starts with the siting in front of the computer, continues when using the internet, and remains after the personal data have been submitted.

Within an extended model of online privacy concern research and based on an intuitive notion that personality certainly determines our everyday life, the aim of this paper is to explore what determines the privacy concern of Internet users and, specifically, if and how their personality shapes and explains the level of their concern about privacy when online.

4 This chapter was published in April 2017 as Škrinjarić, Budak, Žokalj: The Effects of Personality traits on Online Privacy Concern EIZ-WP-1702 http://www.eizg.hr/hr-HR/Radni-materijali-EIZ-a-207.aspx . The upgraded version is forthcoming in Ekonomski pregled 69 (2) in 2018.

The research hypotheses argue whether five personality traits significantly influence an individual's online privacy concern. Based on the theoretical model and intuitive rationale, and only partially on relatively scarce existing literature, we assume a positive impact of conscientiousness, openness and neuroticism on online privacy concern, while extraversion and agreeableness are expected to affect it negatively. The divergence between the theory and empirical evidence is observed in the latter two personality traits which mostly prove to be positively correlated with the level of online privacy concern.

As Li (2011) notes, personality traits are underexplored in the online privacy concern literature and this paper contributes by filling this gap. The fact that so far, to the best of our knowledge, only two papers address this important issue, is enough to motivate us to look further into the potential importance of personality traits for online privacy concern. Studies of Junglas, Johnson, and Spitzmuller (2008) and Korzaan and Boswell (2008), although both examining personality traits and the online privacy concern nexus, are of different size and scope when compared to the comprehensive and extended model applied in this research. The value added is the empirical analysis performed on the large survey of over 2,000 Internet users.

In order to provide plausible answers on how personality traits fit in the privacy story and how they can explain the variations in online privacy concern, one should understand the reasons behind the research of online privacy concern in general, as well as personality traits which are considered to be relevant antecedents. Therefore, the theoretical framework consisting of the Big Five theory of personality traits and online privacy concern is briefly explained in the following chapter. After the literature review and an overview of the hypotheses that will be tested, we proceed with the empirical analysis based on survey data collected in 2016 on a large sample of Internet users in Croatia. The survey sample, data and variables as well as methodology are provided in section three of the paper. The results are discussed in section four and the last section presents conclusions and lines of future research.

6.1. Literature Review

Since the golden age and the breakthrough of computer science, which took place in the last decade of the previous century, the pioneering work arguing the significance of personality differences among individuals was Smith et al. (1996). Personality traits can be defined as "the substance of personality" (McCrae and Costa, 1987), an individual's tendencies resulting in different attitudinal and behavioral patterns across a diverse set of situations. Thus, depending on their personality, individuals' opinions and actions regarding online privacy concern differ. The upside of personality traits in explaining online privacy concern is their hereditary origin (Bergeman et al., 1993), as well as their stability across an individual's lifetime (McCrae and Costa, 1991) and across cultures (Salgado et al., 2003). Given the aforementioned characteristics, one can assume relative invariability of personality traits both through time and across different countries or cultures.

Various theoretical approaches to personality have resulted in different measurements and indicators of an individual's characteristics. In the psychological literature, Tupes and Christal (1961) are recognized as the first authors discovering five-factor personality traits. In pursuit of a unified framework, which would be applicable and accepted in the scientific community, the Big Five framework further emerged in the late 1980s and was developed in different versions (e.g. Goldberg, 1992), ranging from very large 60-variable models to more reduced models (see Donellan et al., 2006 for a review). The Big Five framework divides personality into five traits, namely openness (to experience), conscientiousness, extraversion, agreeableness and neuroticism (sometimes referred to as emotional instability). From the large psychological studies, shortened versions of the Big Five framework have been developed in order to make them suitable for usage in other research fields and when the questionnaire time is limited; for example, there is a highly used abbreviated 10-item version developed by Rammstedt and John (2007).

The aforementioned personality traits are confronted in this paper with online privacy concern (OPC), a construct indicating an individual's level of perceived harm or vulnerability when using the Internet (Malhotra, Kim, and Agarwal, 2004).

Among many potential antecedents, a range of other factors might affect online privacy concern, such as sociodemographic factors, cultural values, computer literacy and others (see for example Chen and Liu, 2015; Ur and Wang, 2013; Ifinedo, 2011). The direction and strength of the relation between demographic characteristics and privacy concern are ambiguous. Most of the studies, however, find that females and the elderly are more privacy-concerned when compared to males and the younger population (for a review, see Anić, 2015).

Another underexplored, yet important determinant of online privacy concern is culture. Bellman et al. (2004) find that some cultural values have effects on privacy concern, but that impact is mediated by the regulatory structure. The effect of societal culture on privacy concern is confirmed by Milberg, Smith, and Burke (2000): power distance, individualism and masculinity have a positive impact on privacy concern, and uncertainty avoidance has negative. Budak, Rajh, and Žokalj (2016) observe differences in individuals' set of values among Internet users in Croatia and suggest more research on the direction and strength of causal relations of values, demographic characteristics and social trust as antecedents of online privacy concern. Social trust is supposed to stand as a key factor in building an individual's trust in institutions and other people. The importance of trust rises in the context of conducting Internet transactions, because of the increased uncertainty and risks related with online transactions (Pavlou, 2002). This goes hand in hand with previous experience of the Internet user or somebody close to him/her that might strongly affect the individual's privacy concern (Okazaki, Li, and Hirose, 2009). Namely, negative experience connected to privacy intrusion, stealing data or simply spams and advertising should considerably alter the privacy concern of the victim.

Privacy awareness is the consciousness of an individual about the importance of privacy and privacy threats. People might or might not be aware of the fact that everything ever posted on the web remains there forever and might be (mis)used. Privacy awareness also involves awareness of privacy policy practices of both government and business sectors. Privacy awareness might have a positive or negative influence on online privacy concern, in particular of consumers (Dommeyer and Gross, 2003). A person who is better acquainted with the privacy policy put in place might see the leakages in the system and that will increase his/her online privacy concern. On the other hand, if a person feels safe and well-informed about privacy protection, he/she should be less concerned about his/her privacy when online. Also, it should be noted that if protective behavior requires slowing down of an individual's online activities or an effort above individual's threshold, it is unlikely that he/she will take it since complete transparency demands no effort (Regan, 2002).

Finally, personal computer skills are expected to be positively related to the online activities of Internet users. People who have better IT knowledge are expected to use the Internet more and for a wider range of operations and this might ease their online privacy concern. Within this context, an eased online privacy concern may emanate as a result of strong privacy protection which is positively correlated to Internet skills (Buchi et al., 2016). In contrast, computer anxiety, described as aversion towards computerization (Parasuraman and Igbaria, 1990), may increase the privacy concern of Internet users. Previous research has found that computer anxiety affects users' performance (Thomas, 1994), so it might lead to increased privacy concern when online.

The following section will further expand on the sample and variable characteristics. Since the research focus is on the personality traits and online privacy concern nexus, the literature review further describes a more narrowed body of the relevant literature.

The impact of personality traits on online privacy concern has been relatively recently examined and provides a lot of potential for future research. Stewart and Segars (2002) tried to develop a first-order and second-order construct of the concern for information privacy

and restated personality traits as one of the antecedents. To the authors' best knowledge, Junglas et al. (2008) is the trailblazing study in this field. Their seminal work certainly integrates the aforementioned theoretical work and empirical research upon which later papers will be based. They investigated the connection between the Big Five and concern for privacy (CFP) in the context of adoption of location-based services. Using a survey-based approach on a sample of 378 undergraduate and graduate students, the authors estimate a structural equation model (SEM) which indicates a positive impact of conscientiousness and openness, and a negative effect of agreeableness on CFP. Neuroticism and extraversion came up insignificant in explaining an individual's concern for privacy.

Korzaan and Boswell (2008) follow the same methodology on a sample of 230 undergraduate students, and find a significant and positive influence of solely agreeableness on concern for information privacy. Bansal et al. (2010) evaluate the impact of the Big Five on perceived health information sensitivity, which is a positively-affecting determinant of health information privacy concern, on a sample of 367 students using SEM. Agreeable and neurotic students are more sensitive regarding their health information, while the opposite stands for the more open ones.

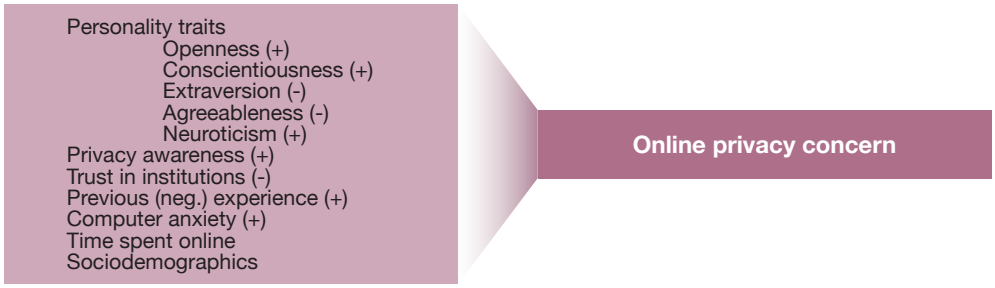
In the context of Facebook activity, Sumner et al. (2011) analyze a survey on a sample of 537 individuals (mostly from the US and the UK) using Spearman correlation. Their results imply a positive effect of extraversion, neuroticism and agreeableness on OPC. Morton (2013) estimates SEM on survey data from 353 students, and constructs two higher-order factors of personality traits, namely stability (agreeableness, conscientiousness, reversed neuroticism) and plasticity (openness, extraversion), concluding a negative impact of stability on concern about the privacy behavior of organizations and government.

Hin et al. (2015) analyze survey data from 291 adults in Malaysia using Pearson correlation. They divide concern for information privacy (CFIP) into four factors – collection, improper access, errors and secondary use – and further investigate the impact of personality traits on each factor. Extraversion and openness correlate positively with collection, the

aforementioned traits and conscientiousness are positively correlated with improper access and errors, while agreeableness and neuroticism are related with secondary use, positively and negatively, respectively. Osatuyi (2015) examines data from 298 undergrads using SEM-PLS and detects a positive impact of agreeableness and conscientiousness on information privacy concern on social media platforms.

Based on the theoretical model and intuitive rationale we will test the hypotheses represented in the conceptual model (Figure 8). A positive impact of conscientiousness, openness and neuroticism on online privacy concern comprises the affirmative set of hypotheses, while a negative effect of extraversion and agreeableness is examined in the two remaining ones.

Figure 8. Conceptual Model of Antecedents to Online Privacy Concern



6.2. Data and Variables in the Model

Data for this paper were collected by computer-assisted telephone interviewing (CATI) method during the period from November 2015 to March 2016. Internet users in Croatia represent the population for this study, and secondary data (provided by Stilus Media) were used to assess the number of Internet users in Croatia. An online phone book was used as a sampling frame. The sample was created based on a one-way stratification by 21 counties. The sample allocated to each stratum was proportional to the assessed number of Internet users in each stratum. Within each stratum a 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 systematic sampling procedure. The final sample consists of 2,060 Internet users aged 18 or older.

The dependent variable in the model is online privacy concern. Although the intensity or range of online privacy concern is subjective and difficult to measure, we have taken the measurement scales developed by Smith, Milberg, and Burke (1996) and described in Malhotra, Kim, and Agarwal (2004), and adapted them for the Internet environment (Table 17). The determinants of online privacy concern have been taken from the existing literature on antecedents of privacy concern and adapted for the online environment.

For personality traits we used the Big Five psychological assessment, based on how well the offered statements describe a respondent's personality regarding openness, conscientiousness, extraversion, agreeableness and neuroticism. The shortened version of the Big Five developed and tested by Rammstedt and John (2007) was employed. It includes self-ratings on whether a person sees him/herself as someone who is reserved, gets nervous easily, is generally trusting, has an active imagination, does a thorough job, is outgoing and sociable.

Openness to experience (henceforth openness) corresponds to an individual's curiosity and propensity towards new experiences. Due to their adventurous and creative mind, individuals with relatively higher openness are more inclined towards art and culture. On the other hand, people who prefer routines, predictability and have a tendency to "go with the flow", score less on this personality trait. It is expected that more open people have a higher level of awareness, due to their diverse life experience, and are more concerned about online privacy since they are aware of the possible threats.

Conscientiousness pertains to an individual's attention to detail, adherence with standards and orientation towards success, excellence and efficiency. Also, conscientious individuals are more goal-oriented, with high levels of self-discipline and deliberation (Costa et al., 1991). Unlike them, people who score less on this trait are likely to procrastinate and have less determination. As with openness, conscientiousness is expected to have a positive sign with respect to privacy concern due to the person's attention to detail.

Extraversion is related to the experience of positive life events and extroverts have generally more friends and acquaintances. Also, they are characterized as energetic and outgoing, and often find themselves in social situations (Judge et al., 2002). On the other hand, introverts have less need for social interaction and are more vulnerable to external threats. In our research, we assume a negative correlation of online privacy concern and level of extraversion.

Agreeableness refers to an individual's empathy towards others through expression of concern and sensitivity. Furthermore, common attributes given to agreeable individuals are soft-heartened, good-natured, cooperative, tolerant and trustful. Thus, the proposed research hypothesis is a negative connection between agreeableness and online privacy concern, since agreeable individuals can be characterized as optimistic people with a strong tendency towards interpersonal relations.

Finally, neuroticism (or sometimes referred to as emotional instability) is a personality trait which manifests itself through frequent mood changes, periods of anxiety and diminished stress management. Also, neurotic persons are much easily irritated, worried and upset. As Junglas et al. (2008) remarked, individuals who score higher on neuroticism are less satisfied with their job. Due to their negative state of mind, we argue a positive correlation with online privacy concern since neurotic persons are (over)aware of the dangers posed by the Internet.

Demographic characteristics of the respondents – in our case Internet users – might explain the level of online privacy concern (e.g. Zhang et al., 2002; Hoy and Milne, 2010), so gender, age, education attained, occupation and size of the household have been included in the model as well. The differences between urban and rural Croatia are difficult to capture by the location of the respondent because urban and rural areas in the sense of development and infrastructure are not clearly delineated. The size of place of residence is more precise variable, yet its effect might be two-fold. In small places people might be more active and free of concerns when online because they have few alternatives in social and cultural life. However, this might be equally true for respondents living in large cities.

Table 17. Variables in the Model

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)
Extraversion (ex)	Index computed from these two items*: - I see myself as someone who is reserved.** - I see myself as someone who is outgoing, sociable. (Cronbach alpha 0.34, inter-item correlation 0.25)
Agreeableness (ag)	Index computed from these two items*: - I see myself as someone who is generally trusting. - I see myself as someone who tends to find fault with others.** (Cronbach alpha 0.03, inter-item correlation 0.01)
Conscientiousness (co)	Index computed from these two items*: - I see myself as someone who tends to be lazy.** - I see myself as someone who does a thorough job. (Cronbach alpha 0.40, inter-item correlation 0.28)
Neuroticism (ne)	Index computed from these two items*: - I see myself as someone who is relaxed, handles stress well.** - I see myself as someone who gets nervous easily. (Cronbach alpha 0.54, inter-item correlation 0.50)
Openness (op)	Index computed from these two items*: - I see myself as someone who has few artistic interests.** - I see myself as someone who has an active imagination. (Cronbach alpha 0.37, inter-item correlation 0.44)
Gender	1 = Male, 0 = Female
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
Household (hh)	Number of people living in respondent's household
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
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
Previous online privacy experience (pe_onl)	Have you or somebody close to you had bad experiences with regard to privacy violation on the Internet before? (1 = Yes, 0 = No)
Trust in institutions (inst_tru)	Index computed from these three items*: - How much do you trust public authorities? - How much do you trust the police? - How much do you trust courts? (Cronbach alpha 0.75, inter-item correlation 0.66)
Time (time)	Number of hours in a typical day the respondent spends on the Internet
Privacy awareness (aw)	Index computed from these five items*: - I am aware of the privacy issues and practices in our society. - I follow the news and developments about privacy issues and privacy violations. - es and the solutions that companies and the government employ to ensure our privacy. - Websites seeking information online should disclose the way the data are collected, processed and used. - A good online privacy policy should have a clear and conspicuous disclosure. (Cronbach alpha 0.66, 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 computerization in my life. (Cronbach alpha 0.72, inter-item correlation 0.82)

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. ** Prior to calculating the index value, these items were recoded as they have reverse direction from that of the latent variable they are estimating.

The items on previous experience were put in rather simple yes or no questions (adapted from Li, 2014). We distinguished negative experiences of the respondents (or somebody close to them) with regard to privacy violation on the Internet, from previous experience with privacy violation in general. Time spent online is used as a proxy for intensity of using the Internet.

To measure trust in institutions, three items were employed: one measuring the general trust in public authorities, and the other two specifically measuring trust in the police and judiciary (Naef and Schupp, 2009). Fear of technology as well as concern about the negative aspects of computerization and frustration related to computer anxiety were measured using the adapted items of Parasuraman and Igbaria (1990).

Table 18 gives a preliminary descriptive view on the characteristics of the sample. Given the sample and the scale from 1 to 5, the average individual is relatively concerned for his/her online privacy concern with a mean value of 3.56. Furthermore, the highest value is achieved in conscientiousness (4.09), thus indicating that the average Croatian respondent is success-oriented as well as self-disciplined and efficient. Relatively high scores of 3.96 and 3.92 are achieved in agreeableness and extraversion, respectively, hence implying a strong social component of the population. The aforementioned characteristics are observable through empathy and trustworthiness, as well as outgoingness manifested in a broad circle of friends and acquaintances. On the other hand, neuroticism and openness scored relatively the lowest, with a mean of 2.47 and 2.87, respectively. As a result, one could argue general preference of the sample towards predictability and routines, instead of creativity and adventure (low openness) and low levels of anxiety, stress and emotional stress.

Even though secondary to the research, interesting conclusions can be drawn from the scores of other variables. It appears that trust in institutions, composed of trust in public authorities, the judiciary and police, is relatively low among the population (a score of 2.75). A plausible explanation behind the lack of trust could lie in the perception of corruption of public bodies, which is often reinforced by the discoveries of malicious practice in law-enforcement, the

judiciary and other public authorities.

The presence of the Internet in everyday life is quantified through the mean of 3.22, thus showing that an average Croatian respondent spends just above three hours a day online. Furthermore, the potential privacy risks emanating from the use of the Internet are generally well-perceived (3.92). Finally, fear of computerization and concern about the pace of automation, both forming computer anxiety, are relatively limited (a mean value of 2.94).

Table 18. Descriptive Statistics, N = 2,060

Variable	Mean	St. Dev.	Min.	Max.
Online privacy concern	3.56	0.96	1	5
Personality traits				
Extraversion	3.92	0.87	1	5
Agreeableness	3.96	0.70	1	5
Conscientiousness	4.09	0.84	1	5
Neuroticism	2.47	0.96	1	5
Openness	2.87	0.86	1	5
Gender*				
Male	0.50	0.50	1	1
Female	0.50	0.50	0	0
Age	39.83	12.91	18	84
Education*				
Primary or less	0.01	0.09	0	1
Secondary	0.50	0.50	0	1
Tertiary	0.46	0.50	0	1
PhD or post-grad	0.03	0.17	0	1
Number of people in household	3.52	1.26	1	12
Occupation*				
Self-employed	0.02	0.14	0	1
Manager	0.02	0.14	0	1
Professional	0.30	0.46	0	1
Technician/clerk	0.18	0.39	0	1
Worker	0.25	0.43	0	1
Retired	0.09	0.28	0	1
Student	0.09	0.28	0	1
Unemployed	0.05	0.22	0	1

Variable	Mean	St. Dev.	Min.	Max.
Other	0.01	0.08	0	1
Size of place of residence*				
10,000 or less	0.14	0.34	0	1
10,001–50,000	0.35	0.48	0	1
50,001–100,000	0.15	0.36	0	1
More than 100,000	0.36	0.48	0	1
Previous experience – online privacy breach	0.18	0.38	0	1
Trust in institutions	2.75	0.94	1	5
Time spent actively online	3.22	2.87	0.5	24
Privacy awareness	3.92	0.64	1.4	5
Computer anxiety	2.94	1.06	1	5

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.

6.3. Results and Discussion

First we use simple OLS regression using the model:

$$opc_i = \alpha + PT_i`\beta + X_i`\delta + \varepsilon_i` ,$$

where online privacy concern is a dependent variable, β is a 5-dimensional vector of estimated coefficients for each of the personality trait (*PT*) dimensions, *X* is a matrix of all other covariates used in the regression, while δ is the vector capturing estimated coefficients of those covariates. All of the latent variables used in the model above (opc, ex ag, co, ne, op, inst_tru, aw and ca) enter the equation in their standardized form, i.e., with a mean of 0 and standard deviation of 1, hence they are interpreted in terms of standard deviations.

The results from the OLS regression are presented in Table 19. In each successive model we add more control variables. Out of five personality trait dimensions, only two showed to be of statistical significance, namely extraversion and neuroticism. A unit standard deviation increase in a person's extraversion characteristic will lead to a decrease of 0.038 standard deviations in their online privacy concern, referencing Model 3 where this showed to be significant. This finding is what we expected. Intuitively, a person who is more extraverted, i.e., more energetic, outgoing and often found in social situations, might be less concerned about their online privacy. In fact, such a person might enjoy sharing private information (in

the form of pictures, attendance at different events, etc.) on various forms of social media.

Turning our attention now to neuroticism, a unit standard deviation increase in a person's neuroticism characteristic will lead to an increase between 0.033 and 0.037 standard deviations in their online privacy concern. This result was also expected. Intuitively, we expect someone who is more neurotic, i.e., has frequent mood changes and gets irritated easily, to be more concerned about their online privacy. Such people may decide to share as little information online (or with other people) as possible because revealing something personal might be the cause of their neuroticism in the first place.

Further analyzing the results presented in Table 19, we can see that neither gender, age, nor number of people in the household affect a person's degree of online privacy concern. The same can be said for the respondent's educational level, occupation, place of residence and trust in institutions. It is interesting to notice that time spent online during a day (time) also plays no role in determining online privacy concern. At first glance one might expect that people who spend most of their time online get more experienced about different aspects of Internet use and personal information protection, so they might be less concerned about their privacy. However, the other side of the coin is that those people might become increasingly aware of potential dangers lurking beneath those codes of ones and zeros. The latter explanation might actually be more relevant to our case, as we find a strong statistical significance of previous online privacy breaches for the current level of online privacy concern (opc is increased by 0.267 standard deviations if the respondent had previous negative experience with online privacy breach).

Two other variables that showed to be statistically significant are privacy awareness and computer anxiety, both positively affecting the level of privacy concern when online.

Analyzing the former, it is not hard to imagine that those who keep themselves updated (aware) about various data gathering policies and privacy-related issues on the Internet are more concerned about their privacy when online. However, the strongest effect on online

privacy concern comes from the latter – one standard deviation increase in computer anxiety is translated into an increase of 0.423 to 0.440 standard deviations in online privacy concern. Intuitively, people who think that the pace of computerization nowadays is dangerously high and represents a threat to privacy in this country are more likely to be worried about the information they provide online.

Table 19. OLS Estimation Results

	Model 1		Model 2		Model 3	
Extraversion	-0.029	(0.020)	-0.031	(0.020)	-0.038*	(0.020)
Agreeableness	-0.030	(0.021)	-0.029	(0.021)	-0.024	(0.021)
Conscientiousness	0.030	(0.020)	0.024	(0.021)	0.017	(0.021)
Neuroticism	0.032	(0.020)	0.037*	(0.020)	0.033*	(0.020)
Openness	-0.020	(0.019)	-0.020	(0.020)	-0.022	(0.020)
Privacy awareness	0.212***	(0.020)	0.208***	(0.020)	0.204***	(0.020)
Computer anxiety	0.440***	(0.019)	0.434***	(0.020)	0.423***	(0.020)
Male			-0.013	(0.039)	-0.014	(0.039)
Age			0.001	(0.002)	0.001	(0.002)
Household			0.019	(0.015)	0.021	(0.015)
Education effect (benchmark is primary education)						
Secondary			-0.095	(0.137)	-0.151	(0.139)
Tertiary			-0.139	(0.140)	-0.202	(0.142)
Post-grad			-0.017	(0.176)	-0.092	(0.179)
Occupation effect (benchmark is self-employed)						
Manager			-0.025	(0.178)	0.002	(0.178)
Professional			-0.020	(0.126)	-0.003	(0.126)
Technician			0.027	(0.124)	0.039	(0.124)
Worker			0.075	(0.122)	0.072	(0.121)
Retired			0.011	(0.143)	0.025	(0.142)
Student			-0.138	(0.132)	-0.128	(0.132)
Unemployed			-0.066	(0.142)	-0.053	(0.141)
Other			0.014	(0.258)	0.015	(0.257)
Size of place of residence effect (benchmark is less than 10,000)						
10,001–50,000			0.018	(0.060)	0.012	(0.060)
50,001–100,000			0.008	(0.071)	0.012	(0.070)
> 100,000			0.042	(0.060)	0.029	(0.060)
Previous online experience					0.267***	(0.051)

	Model 1	Model 2	Model 3	
Trust in institutions			-0.021	(0.020)
Time			-0.002	(0.007)
N	2,060	2,060	2,060	
Adj. R^2	0.2592	0.2590	0.2689	
Notes: Standard errors in parentheses; * p < 0.10, ** p < 0.05, *** p < 0.01.				

The analysis thus far has been carried out on standardized outcome variables and most of the interpretations are expressed in terms of standard deviations. Although this is statistically very well-ordered, intuitively it might be difficult to grasp. With that in mind, and also as a robustness check, we also run an ordered probit model to assess the probability of getting each possible outcome of the online privacy concern (opc) variable.

In the ordered probit model, we assume the underlying relationship as

$$y^*_i = X\,\alpha_i`\beta + \varepsilon_i\ ,$$

where dependent variable y^* is exact but unobserved – instead, we can only observe different categories $j \in \{1, 2,..., M\}$ of this variable, and we define thresholds α such that

$$y_i = j \text{ if } \alpha_{j-1} < y^*_i \leq \alpha_j\ ,$$

Then, the probability that the observation i will choose alternative j is given by

$$p_{ij} = p\,(y_i = j) = p\,(\alpha_{j-1} < y^*_i \leq \alpha_j) = F\,(\alpha_j - X_i`\,\beta) - F\,(\alpha_{j-1} - X_i`\,\beta)\ ,$$

where F is standard normal cumulative distribution function. The model is estimated using maximum likelihood.

In our case, the online privacy concern (opc) dependent variable can take five different categories (outcomes), as described in Table 20. These outcomes were obtained by rounding the value of the opc variable to the nearest whole number for each respondent.

Table 20. Online Privacy Concern Variable Labels

opc outcomes	Label
1	Not concerned at all
2	Unconcerned
3	Neither concerned nor unconcerned
4	Concerned
5	Very concerned

All of the latent covariates (ex ag, co, ne, op, inst_tru, aw and ca) still enter the equation in their standardized form and are hence interpreted in terms of standard deviations, but the dependent variable opc now enters as a discrete variable. Table 21 shows the results of ordered probit estimations.

Table 21. Ordered Probit Estimation Results

	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
Extraversion	0.001 (0.000)	0.007* (0.004)	0.009* (0.005)	-0.006* (0.003)	-0.011* (0.007)
Agreeableness	0.000 (0.000)	0.000 (0.004)	0.000 (0.006)	0.000 (0.003)	-0.000 (0.007)
Conscientiousness	-0.000 (0.000)	-0.005 (0.004)	-0.006 (0.005)	0.004 (0.003)	0.008 (0.007)
Neuroticism	-0.001* (0.000)	-0.008* (0.004)	-0.010* (0.005)	0.006* (0.003)	0.012* (0.007)
Openness	0.000 (0.000)	0.006 (0.004)	0.008 (0.005)	-0.005 (0.003)	-0.009 (0.006)
Privacy awareness	-0.003*** (0.001)	-0.040*** (0.005)	-0.051*** (0.006)	0.032*** (0.004)	0.063*** (0.007)
Computer anxiety	-0.007*** (0.001)	-0.083*** (0.006)	-0.106*** (0.007)	0.065*** (0.006)	0.129*** (0.007)
Male	0.000 (0.001)	0.003 (0.008)	0.004 (0.010)	-0.003 (0.006)	-0.005 (0.013)
Age	0.000 (0.000)	0.000 (0.000)	0.001 (0.001)	-0.000 (0.000)	-0.001 (0.001)
Household	-0.000 (0.000)	-0.000 (0.003)	-0.000 (0.004)	0.000 (0.003)	0.000 (0.005)
Education effect (benchmark is primary education)					
Secondary	0.004*** (0.001)	0.072*** (0.016)	0.158*** (0.056)	0.005 (0.039)	-0.239** (0.108)
Tertiary	0.005*** (0.001)	0.082*** (0.017)	0.170*** (0.057)	-0.003 (0.038)	-0.254** (0.110)
Post-grad	0.004* (0.002)	0.074*** (0.028)	0.161** (0.064)	0.004 (0.042)	-0.243** (0.115)
Occupation effect (benchmark is self-employed)					
Manager	0.002 (0.002)	0.023 (0.034)	0.036 (0.053)	-0.015 (0.022)	-0.046 (0.068)
Professional	0.002 (0.002)	0.027 (0.024)	0.040 (0.041)	-0.017 (0.013)	-0.051 (0.054)
Technician	0.002 (0.002)	0.033 (0.024)	0.049 (0.041)	-0.023* (0.013)	-0.061 (0.053)
Worker	0.001 (0.001)	0.017 (0.023)	0.027 (0.041)	-0.010 (0.012)	-0.034 (0.054)
Retired	0.001 (0.002)	0.022 (0.027)	0.034 (0.044)	-0.014 (0.016)	-0.044 (0.057)
Student	0.006** (0.003)	0.074** (0.029)	0.089** (0.042)	-0.059*** (0.021)	-0.110** (0.055)
Unemployed	0.004 (0.002)	0.046 (0.030)	0.063 (0.044)	-0.034 (0.020)	-0.079 (0.057)
Other	-0.000 (0.003)	-0.002 (0.042)	-0.003 (0.076)	0.001 (0.020)	0.004 (0.102)
Size of place of residence effect (benchmark is less than 10,000)					

	Outcome 1	Outcome 2	Outcome 3	Outcome 4	Outcome 5
10,001–50,000	0.000 (0.001)	0.001 (0.012)	0.002 (0.016)	-0.001 (0.010)	-0.002 (0.020)
50,001–100,000	0.001 (0.001)	0.010 (0.015)	0.013 (0.019)	-0.008 (0.012)	-0.016 (0.023)
> 100,000	0.000 (0.001)	0.004 (0.013)	0.005 (0.017)	-0.003 (0.010)	-0.006 (0.020)
Previous online experience	-0.004*** (0.001)	-0.052*** (0.011)	-0.067*** (0.014)	0.041*** (0.009)	0.082*** (0.017)
Trust in institutions	0.001** (0.000)	0.010** (0.004)	0.013** (0.005)	-0.008** (0.003)	-0.016** (0.006)
Time	0.000 (0.000)	0.001 (0.001)	0.002 (0.002)	-0.001 (0.001)	-0.002 (0.002)
N	2,060	2,060	2,060	2,060	2,060

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

We start interpreting these results by confirming that only two dimensions of personality traits are statistically significant in explaining variation in online privacy concern – extraversion and neuroticism. Starting with the interpretation of the former covariate, an increase of one standard deviation in extraversion from the mean is estimated to lead to a 0.7 and 0.9 percent increase in probability to be unconcerned or neither concerned nor unconcerned for online privacy, respectively. However, for the last two outcomes, the signs of the relationship are reversed – an increase of one standard deviation in extraversion from the mean is estimated to lead to a 0.6 and 1.1 percent decrease in probability to be concerned or very concerned for online privacy, respectively. These findings are consistent with the previous results from the simple OLS model, i.e., people with more characteristics of an extrovert are less likely to be concerned about their online privacy.

Looking at the results for the neuroticism personality trait, we can see that a unit standard deviation increase from the mean in this variable leads to a decrease in probability of being not concerned at all, unconcerned or neither concerned nor unconcerned for online privacy by 0.1, 0.8 and 1.0 percent, respectively; and to an increase in probability of being either concerned or very concerned for online privacy by 0.6 and 1.2 percent, respectively. This is also consistent with our previous results, i.e., less emotionally stable people tend to be more concerned about what information they are providing in an online environment.

It is interesting to see that some education and occupation effects become significant in this case. Referring first to the latter, only students exhibit statistically significant effects for all five possible outcomes. Compared to the people who are self-employed, students are more prone to be not concerned at all (0.6 percent) or unconcerned (7.4 percent), and less likely to be concerned (-5.9 percent) or very concerned (-11.0 percent) about their online privacy. This can be justified by the fact that students are those who use the Internet and various forms of social media -mostly for recreational and educational purposes. These are young people who have been using information technology since their childhood, and communicating, shopping, studying, posting on Facebook, tweeting, browsing through YouTube videos and other forms of entertainment are their way of life.

The education effect is also highly significant. Compared to someone with only primary education, every additional education degree obtained – secondary, tertiary and post-grad – decreases the likelihood of being very concerned for online privacy by 23.9, 25.4 and 24.3 percent, respectively. These people are most likely to be neither concerned nor unconcerned about their online privacy – this is the case for 15.8 percent of secondary school graduates, 17.0 percent of university graduates and 16.1 percent of people with a master's or doctoral degree. The rationale here is that as people become more educated, they also become more familiar with Internet use, as they have likely used it very frequently during their education process, and it becomes only natural to use the Internet for everyday purposes.

Another variable that becomes significant is trust in institutions, and the obtained results suggest that an increase in this trust is most likely to result in people being unconcerned (1 percent) or neither concerned nor unconcerned (1.3 percent) about privacy while online. This is to be expected, since an effective judiciary system, coupled with unbiased police interventions and uncorrupt public authorities, provides a sense of security even in the online environment. Existence of previous online privacy breach leads to higher levels of online privacy concern, with the most likely outcome of being very concerned (8.2 percent likelihood).

Gender, age, size of place of residence, number of people in the household and time spent actively online all showed to be insignificant.

6.4. Conclusion

This empirical study sheds light on the effect of personality on privacy concern, specifically in the online environment, which is seen as a contribution to the existing research on this topic. In particular, the comprehensive approach of including other latent variables as antecedents to online privacy concern is considered a novelty, and findings are robust due to the large dataset employed. The analysis indicates that an average Internet user in Croatia is concerned about privacy when online, and that the Croatian Internet population is very conscientious, agreeable and extraverted. The positive effect of conscientiousness on online privacy concern was not significant. This might indicate that no matter how Internet users are efficient, self-disciplined and responsible in their work and in timely completing their tasks and duties, they might share concerns about privacy when online. Although openness has been assumed and confirmed in previous studies to be positively related to privacy concern, this was not confirmed in this research. Actually, the positive relation is somehow counter-intuitive because one would assume that more open people would not care much about their privacy. Although this antecedent has a negative coefficient, the relationship is not significant. As expected, but opposite to previous findings of Junglas et al. (2008), neuroticism and extraversion came up significant in explaining an individual's concern for privacy. The ambiguous effect of agreeableness in the literature has not been resolved either way in this empirical study. However, this research clearly shows that certain personality traits of Internet users determine the level of their concern about online privacy. The more extraverted and neurotic a person is, the more concerned about online privacy he/she is.

The main purpose of this paper is to test whether personality stands as an antecedent of online privacy concern and whether it should be included in the extended model of online privacy concern. However, the analysis conducted on a large sample has also enabled us to learn more about the personality traits of Internet users in Croatia and this might be used for other studies as well. For example, getting more in-depth insight into the personality of

Internet users in the context of their online privacy concern might be useful in designing marketing strategies and consumer-oriented business policies.

Although the empirical analysis uses a large set of nationwide individual data, which is considered a scientific contribution to the existing research, the survey was conducted on only one country's Internet user population. We recognize this as a limitation of the research that might also be seen as a potential for extending the research to other nations by using the same methodology and survey instrument. Another line of future research is to test the extended model of online privacy concern with the consequences of online privacy concern included in the model.

7. THE ROLE OF CONSUMER-RELATED AND REGULATORY CONTROL FACTORS IN ONLINE PRIVACY CONCERN[5]

As the capabilities of digital technologies in collecting, storing and trading of personal data are growing, Internet has become an important marketing tool (Lwin, Wirtz, and Williams, 2007). For marketers, consumer personal data are very valuable, while at the same time the potential loss of those data is considered to be one of the biggest risks to modern business (The Futures Company, 2012). Intense sharing, gathering and manipulation of customers' information have further intensified the issue of privacy concern in online commercial setting. Many studies show that consumers have become more concerned about data privacy in recent years (Pingitore et al., 2013). In online transactions, individual consumers have usually little power and less control over the use of their personal data (The future of company, 2012) and privacy concern is particularly evident in situations where personal data are shared in one context and used by companies for other, commercial purposes. Misuse of personal data and illegal activities on the Internet further intensify privacy concern, while businesses and regulators are responding slowly when it comes to protecting consumers. As a result of all potential privacy threats, many Internet users may take counter measures to protect their privacy (Lwin, Wirtz, and Williams, 2007), which negatively affects e-commerce (Malhotra, Kim, and Agarwal, 2004). The key issue in privacy literature is to find the way to reduce privacy concern and increase consumer confidence in using the Internet. In this sense, understanding the antecedents of privacy concern is the basis for developing more effective privacy policies.

The purpose of this chapter[6] is to examine and compare the impact of demographic factors, control variables and perception of the effectiveness of government online regulation on online privacy concern (hereafter OPC). The analysis was done on a representative sample

5 Ivan-Damir Anić and Vatroslav Škare.

6 This chapter is based on the paper presented at the International CIRCLE Conference Creating and Delivering Value, April 19-21, 2017, Poland: Warsaw. Abstract was published in the Book of abstracts as Anić, Ivan-Damir; Škare, Vatroslav. Online Privacy Concern in Croatia: the Effect of Consumer- and Regulatory Control Factors, 14th International CIRCLE Conference "Creating and Delivering Value", Ryding, Daniella; Krzyzanowska, Magdalena, editor(s). Lancashire: Access Press, 2017. pp 88-89.

of adult population (N = 2.060) in Croatia. This research integrates in one model three groups of antecedent factors that generated interest in previous research, and provides recommendations for companies and policy makers.

In section 7.1 literature review is presented, followed by methodology in section 7.2. The results are given in section 7.3. The chapter concludes with discussion and conclusions in section 7.4.

7.1. Literature review

Online privacy concern can be defined as individuals' apprehension and uneasiness over the use of their personal data (Westin, 2003; Lwin, Wirtz, and Williams, 2007). Previously, privacy was defined as a fundamental right for humans, while over the years its meaning has developed within society. In online transactions, "the right to be left alone" has developed into the trade-off in which the risks related to costs of user data are evaluated against the benefits of participating in the interaction (Ranzini et al., 2017). In this research we examine consumer privacy in a commercial setting, which is a subset of privacy and it involves physical space, information and a continuum. Consumers have varying degrees of concern about privacy and place different values on their personal information, and thus they may be willing to trade information for a more valued incentive (Caudill and Murphy, 2000).

With respect to antecedents to privacy concern, past research has examined the impact of demographic variables, ethical, legal, regulatory and public policy factors. Among demographic variables, the most frequently studied factors are gender, age, income and education (Li, 2011). Many studies suggest that women tend to be more concerned about their online privacy than men (Sheehan, 1999; O'Neil, 2001; Graeff and Harmon, 2002; Grubbs Hoy and Milne, 2010; Li, 2011; Mathiyalakan et al, 2014; Anić, Škare, and Kursan Milaković, 2016), although a few studies argue that there are no significant differences (Milne and Boza, 1999; Zukowski and Brown, 2007; The Lares Institute, 2011; Zhang, Chen, and Lee, 2013). There are several factors that might explain these findings. Men are more interested in computers; have more computer skills and are more willing to take risks (Sheehan, 1999;

Graeff and Harmon, 2002; Fogel and Nehmad, 2009; Zhang, Chen, and Lee, 2013), while women are more likely to be exposed to online abuse (Grubbs, Hoy, and Milne, 2010). Therefore, the following hypothesis is proposed: H1: As compared to men, women are more concerned about online privacy.

Age was also shown to be related to OPC. Past research suggests that older Internet users tend to be more concerned about privacy than younger ones (Milne et al, 1996; Milne and Boza, 1999; Graeff and Harmon, 2002; Zukowski and Brown, 2007; Zhang, Chen, and Lee, 2013). Younger individuals are more positive and more aware of data collection practices and of financial benefits obtained from online marketing programs (Zukowski and Borwn, 2007), while older users are more sensitive and want to control the usage of their information (Milne, Beckman, and Taubman, 1996; Graeff and Harmon, 2002; Zukowski and Brown, 2007). Therefore, the following hypothesis is proposed: H2: As compared to younger Internet users, older individuals are more concerned about their online privacy.

There are fewer studies that have examined the link between income, education and OPC. Past research shows that individuals with higher income tend to be less concerned about their privacy than low-income consumers (Milne, Beckman, and Taubman, 1996; Milne and Boza, 1999; O'Neil, 2001; Graeff and Harmon, 2002; Zukowski and Brown, 2007; Zhang, Chen, and Lee, 2013), and therefore, the following hypothesis is proposed: H3: There is a negative relationship between income and online privacy concern. With respect to education, previous studies show that less educated individuals have the highest level of concern about online privacy (O'Neil, 2001), and therefore, the following hypothesis is proposed: H4: There is a negative relationship between education and online privacy concern.

Past research analysed consumers' willingness to provide private information to marketers as the consequence of privacy concern, while this research examines the impact of individuals' tendency towards sharing private information online on OPC, which is a measure how acceptable is for him or her to share their private information online. As some individuals are more prone to share their information than the others, it might be assumed that this link is not

so straightforward. We suppose that if an individual is more prone to share information, it is more likely that he or she will express lower level of OPC. Past research suggests that there is a negative relationship between privacy concern and willingness to provide information (Nam et al., 2006; Phelps, D'Souza, and Nowak, 2001; Bandyopadhyay, 2011). Therefore, the following hypothesis is proposed: H5: Tendency towards sharing private information online has negative impact on OPC.

Past research also shows that consumer privacy depends on consumers' ability to control their information in a marketing transactions and the degree of their knowledge of the process (Caudill and Murphy, 2000). In this research, we examine individual's desire for more or less control over collection, sharing and usage of private information as an antecedent to OPC. Past research examined the impact of individual's perceived control (Milne and Boza, 1999), perceived ability to control information (Dinev and Hart, 2004), and individual's desire for information control. The theory posits that the more control an individual desires, the greater his or her privacy concern is (Phelps, D'Souza, and Nowak, 2001). Therefore, the following hypothesis is proposed: H6: Desire for information control is positively related to OPC.

Finally, this research examines the impact of perceived effectiveness of government online regulation on OPC, which is an important issue. On the one hand, the knowledge of Internet users and their resources to secure their data is limited, while on the other hand, government regulation needs to ensure the well-being of consumers and data protection on the Internet (Rust, Kannan, and Peng, 2002; Lwin, Wirtz, and Williams, 2007). Past research suggests that perceived effectiveness of regulatory policies and their enforcement have impact on privacy concern, in a way that weak and less effective perceived government online privacy regulation is related to higher level of privacy concern, which results in higher likelihood that an individual will take counter measures on the Internet to protect his or her privacy (Lwin, Wirtz, and Williams, 2007). Therefore, the following hypothesis is proposed: H7: There is negative relationship between perceived government online privacy regulation and online privacy concern.

7.2. Methodology

The data were collected by survey of Internet users that was carried out during the period of November 2015 – March 2016 in Croatia. The final sample consists of 2,060 Internet users. Sample characteristics are presented in Table 22.

Table 22. Sample characteristics, N=2,060

Variable	N	%
Gender		
Male	1,024	49.7
Female	1,036	50.3
Age		
18 - 24	266	12.9
25 - 34	497	24.1
35 - 44	568	27.6
45 - 54	405	19.7
55 - 64	241	11.7
60+	83	4.0
Income		
up to 2,500 HRK	51	2.5
2,501-5,000 HRK	356	14.8
5,001-7,500 HRK	807	21.9
7,501-10,000 HRK	1,408	29.2
10,001-12,500 HRK	1,682	13.3
12,501-15,000 HRK	1,879	9.6
more than 15,000 HRK	51	8.8
Education		
primary school or less	17	0.8
secondary education	1,035	50.2
tertiary educ. / high school, university	945	45.9
master degree / Ph.D	63	3.1

Note: 1EUR= 7.5HRK (Croatian kuna). www.hnb.hr Source: Survey of Internet users.

The questionnaire included questions about online privacy concern (OPC), demographic variables, tendency towards sharing private information online (SH), individual's desire for

information control (CTRL), and perceived government online privacy regulation (REG). Online privacy concern (OPC) items were taken from study by Smith, Milberg, and Burke (1996). It includes various aspects of individual's online privacy concern, including usage of information, collection and importance of privacy. Items related to OPC were measured on a Likert-type scale, ranging from 1 (strongly disagree) to 5 (strongly agree).

Tendency towards sharing private information online (SH) was measured by asking respondents how acceptable is for them to share online private photos, private information, post their current location, appointments, and share credit card data when they purchase online. Items related to SH were measured on Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree).

Desire for information control (CTRL) was measured with four items related to individual's desire, inclination towards the control of the collection, usage, and sharing of their personal data on the internet, based on past studies (Malhotra, Kim, and Agarwal, 2004; Smith, Milberg, and Burke, 1996). Items related to CTRL were measured on a Likert-type scale, ranging from 1 (strongly disagree) to 5 (strongly agree).

Perceived government online privacy regulation (REG) was measured on three items. Respondents were asked to evaluate if existing policies related to the Iternet are efficient enough to protect people; if government is doing enough to protect people, and if users think there should be stricter government regulation towards the protection of individual's online privacy, based on Lwin, Wirtz, and Williams (2007).

Gender (GEN) of the respondent was coded as 1 for males and 2 for females; Age of the respondent (AGE) as: (1) 18-24, (2) 25-34, (3) 35-44, (4) 45-54, (5) 55-64, (6) 65+; income (INC) as: (1) up to 2,500 HRK, (2) 2,501-5,000 HRK, (3) 5,001-7,500 HRK, (4) 7,501-10,000 HRK, (5) 10,001-12,500 HRK, (6) 12,501-15,000 HRK, (7) more than 15,000 HRK, and education (EDU) as, (1) primary school or less, (2) secondary school, (3) faculty education, (4) Master/ Ph.D. degree).

In order to test the proposed hypotheses, variance-based structural equations modelling (SEM) was used, by means of SmartPLS 2.0 (Ringle, Wende, and Will, 2005).

7.3. Results and discussion

7.3.1. Measurement Model Assessment

All variables in the model were identified reflectively. Table 23 presents the results of assessment of the measurement model. Composite reliability scores and Cronbach's alphas indicate high levels of internal consistency, while the average variances extracted (AVE) signal sufficient convergent validity. During the assessment of internal consistency one item for tendency towards sharing private information online (SH) was omitted because of low indicator loadings.

Table 23. Assessments of the measurement model

	AVE	Composite Reliability	Cronbach's Alpha	R^2
AGE	1.0000	1.0000	1.0000	
CTRL	0.6399	0.8765	0.8140	
EDU	1.0000	1.0000	1.0000	
GEN	1.0000	1.0000	1.0000	
INC	1.0000	1.0000	1.0000	
OPC	0.5720	0.8887	0.8522	0.2193
REG	0.5755	0.8022	0.6718	
SH	0.7123	0.9079	0.8638	

Source: Survey of internet users and authors' calculations.

All latent variables meet the Fornell-Larcker criterion of discriminant validity (Fornell and Larcker, 1981), as presented in Table 24.

Table 24. Assessment of discriminant validity

	AGE	CTRL	EDU	GEN	INC	OPC	REG	SH
AGE	1.0000	0	0	0	0	0	0	0
CTRL	0.1594	0.7999	0	0	0	0	0	0
EDU	0.0307	-0.1041	1.0000	0	0	0	0	0
GEN	0.0394	0.1098	0.0253	1.0000	0	0	0	0
INC	-0.0530	-0.0975	0.3008	-0.0543	1.0000	0	0	0
OPC	0.0862	0.3806	-0.1054	0.0705	-0.0924	0.7563	0	0
REG	-0.0839	-0.2695	0.1194	-0.0544	0.0905	-0.3266	0.7586	0
SH	-0.3282	-0.2285	0.0403	-0.0909	0.0241	-0.2431	0.1902	0.8440

Note: The squared root of AVE is depicted along the diagonal of the correlational matrix.
Source: Survey of internet users and authors' calculations.

7.3.2. Structural Model Results

The coefficient of determination (R2) for the endogenous variable (OPC) is 0.2193, which signals a moderate predictive power of the model. Following the non-parametric bootstrapping procedure (Hair, Hult, Ringle and Sarstedt, 2014), three path coefficients were found to be significant at 99% level, while two path coefficients were significant at 90% level. Two remaining path coefficient were found not to be significant. Results of the structural model are presented in Table 25.

Table 25. Results of the structural model and hypotheses testing

	Path coefficients	Hypotheses testing
GEN -> OPC	0,0146 n.s.	H1 rejected
AGE -> OPC	-0,025 n.s.	H2 rejected
INC -> OPC	-0,0317*	H3 rejected
EDU -> OPC	-0,0340*	H4 rejected
SH -> OPC	-0,1414***	H5 confirmed
CTRL -> OPC	0,2855***	H6 confirmed
REG -> OPC	-0,2172***	H7 confirmed

Note: Significance-level (one-tailed): *p<0.1, ***p<0.01

Source: Survey of internet users and authors' calculations.

The R2 score and the magnitude of the path coefficients reveal that CTRL, REG and SH are the most important factors in the model that affect OPC. As expected, CTRL has a positive effect on OPC, which confirms hypothesis H6. In other words, if individuals desire more control over their private information, OPC will increase. REG is the second most important factor that affects OPC. The results indicate that the weaker (less effective) the perceived government online privacy regulation is, the higher the degree of privacy concern, which supports hypothesis H7. SH is the third the most important factor and, as expected, if individuals are prone to share their private information online, their OPC will be lower, which supports hypothesis H5. Meanwhile, both gender (GEN) and age (AGE) demonstrated no significant effect on OPC, which rejects hypotheses H1 and H2. Finally, as expected income (INC) and education (EDU) are negatively related to OPC, but due the low magnitudes of influence and significance levels of $p<0.1$, hypotheses H3 and H4 are rejected.

7.4. Conclusion

The results of this study show that Internet users have higher level of OPC in the Croatian online environment. At the same time, respondents think that if they have control of information, their privacy will be safeguarded. Higher level of the desire for a higher level control of their personal information increases OPC, which is in line with past research (Phelps, D'Souza, and Nowak, 2001). Second most important factor that influences OPC is perceived government online privacy regulation. Respondents perceive that existing regulation is not effective enough, which means that weaker government online privacy regulation has negative effect on OPC. This finding is also consistent with past research (Lwin, Wirtz, and Williams, 2007). In Croatian online environment, the level of OPC also depends on tendency towards sharing private information (SH). If individuals are more prone towards sharing private information, OPC will be lower. In Croatian environment SH is low. Finally, the results of this research show that there is no significant difference ($p>0.05$) among Internet users in OPC with respect to demographic variables. Therefore, this research confirms that demographics are less important in explaining OPC than other control and regulation variables.

Based on these findings, this study supports the view that government intervention in the

enforcement of more stringent data protection measures on businesses is necessary, at least in the Croatian environment. As consumer perceptions about regulatory environment are low, government should manage privacy in a more responsible manner if they wish to avoid negative actions by consumers. Government may provide their citizens more control over their personal information, and policy efforts to improve privacy protection should be also clearly communicated to the public.

Companies should also work in the direction of providing more control to individuals regarding how their information is collected, used and shared. Marketers should adopt a proactive stance in alleviating OPC and promote privacy policy better. Providing visitors with clear information about the website's privacy policies is one way that companies might mitigate privacy concern, and thus enhance customer satisfaction, trust and customer value.

Although this study provided interesting results, it has also some limitations. The coefficient of determination (R^2) was not high, but it was high enough to help us obtain more insights into proposed relationships among variables. Future studies might expand this model with outcome variables, such as the attitudes towards shopping, intention to buy and purchases over the internet, as well as consumer protective behaviour measures. The model could be also tested in various environments, such as cities, suburban and rural areas. Finally, more studies are needed to test the model in developing countries.

One such extension of the research has been perfomed within PRICON project. It deals with consumers intentions to transact online, depending on their level of privacy concern. The entire research is available in doctoral dissertation of Vedran Recher, 'The Effect of Privacy Concern on Consumer Behavioral Intention in the Online Environment'. Main findings are described in the extended summary of doctoral dissertation presented in the following subchapter.

7.5. Consequences of Privacy Concern: Consumer Behavioral Intention in the Online Environment

Sudden and steep growth in digital technologies and dramatic increase in Internet access in the 21st century revived the interest in privacy issues, which were originally discussed at the end of 19th century due to the invasion of privacy by popular media. With new technologies, these discussions also attained some previously unimaginable layers. The phenomenon and ubiquity of online environment in the developed world has deepened the issue of consumer privacy and exposed new questions connected to consumer behavior in the online environment. What determines the consumer privacy concern in online environment, how the consumer online privacy concern affects their behavioral intentions in the online environment and are their differences in this relationship with regards to observed and unobserved characteristics of consumers, are just some questions of interest for businesses, consumers and regulators responsible for consumer online privacy protection. The main goal of this dissertation, which directly follows from these questions, is to investigate the determinants of consumers' online privacy concern and estimate its impact on behavioral intention of consumers in online environment.

Research is conducted on 2,060 survey participants in Croatia, using the partial least squares path modelling. Four determinants were found to have significant impact on online privacy concern: belief in privacy rights, perceived level of data gathering, perceived quality of regulation and social awareness. However, robust effect independent on model specification is found only for belief in privacy rights and perceived level of data gathering. Furthermore, the hypothesis that the main impact of online privacy concern on consumer behavioral intention is indirect is confirmed. Namely, risk perception is the mediating variable between online privacy concern and consumer behavioral intention. Also, age was found to be significant determinant of consumer behavioral intention. Generally, when observing the demographic characteristics of consumers, the differences in online privacy concern were found by age groups and gender, while education does not yield any differences in the level of privacy concern.

Additional important result is found in impact of perceived benefits of using the Internet on consumer behavioral intentions in the online environment. This effect, when looking just the direct effects, is stronger than the impact of online privacy concern on consumer behavioral intention. However, when looking at the sum of indirect and direct effects, in the context of privacy calculus, it is confirmed that online privacy concern has the potential to hamper the growth and development of online companies.

Stated results of the research have implications in terms of doing business in the online environment. First, there is clearly a need to implement larger transparency in data gathering, its purposes and scale. Explicit communication of needed private information which is saved could directly influence exceptionally high level of perceived data gathering. Second, including the tools for decreasing the consumer perceived risk is also highly recommended, due to the fact that perceived risk is the main mediator through which the effect of online privacy concern is being realized. This could be achieved by informing and teaching the consumers about good and ethical business practices of online companies. Third, communication should largely be targeted towards older consumers. In this way, online companies could maximize their potential since older consumers are rarely involved in online transactions, compared to their younger counterparts.

Analysis yielded some indication of influence of regulatory framework and level of online privacy concern. However, recent reform of privacy protection law in the European Union already puts strong emphasis on protection of consumers' interests. It will be interesting in the future to observe the impact of this reform on consumer attitudes, in the context of interactions addressed in this dissertation[7].

7 Doctoral dissertation V. Recher: 'Utjecaj zabrinutosti za privatnost na namjeru ponašanja potrošača u online okruženju' in Croatian language is available upon request. https://bib.irb.hr/prikazi-rad?&rad=908882

8. CITIZENS' ONLINE SURVEILLANCE CONCERN IN A POST-COMMUNIST COUNTRY[8]

Living in the digital age sheds an entirely new light on the surveillance. We live in a surveillance society, as David Lyon noted more than 20 years ago (Lyon, 1994), and surveillance is still a hot issue in post-communist countries. However, research on contemporary surveillance issues in post-communist societies is scarce (see for example Webster et al., Eds. 2011). This paper aims to fill the gap in the body of the research by offering empirical study on surveillance concern, online environment and post-communist context.

In the global digitalized world, the surveillance seems to have no boundaries in the online environment. The literature on surveillance and Internet is rather scarce relative to the wide range of aspects that should be explored. Some studies noted that 'the internet contributes to ever-increasing levels of surveillance' (Whitson, 2010, p.243) due to the inter alia surveillant features of Internet technologies (Wall, 2006).

Allmer (2012) offers the systemized review of Internet surveillance studies and Internet surveillance definitions and elaborates on the economic purpose of Internet surveillance. Built on the premise that Internet surveillance exists, our motif was to investigate how an Internet user in a post transition, post-communist country deals with it, in terms of the level of surveillance concern expressed, and actions taken. It is almost impossible to find a single person in a post-communist European country who lives completely isolated from the Internet. Even if an individual for example does not browse the Internet and doesn't have a smartphone, he/she maybe lives in the video surveilled neighbourhood or has to use an electronic ID pass to enter the workplace building. In 2016, the percentage of regular Internet users in Croatia - the post-communist country we observe in this study - was 71 percent, which is close to the EU average of 79 percent (DESI, 2017).

When online, Internet users are exposed to monitoring and surveillance, but it is not clear

8 The improved version is under consideration for publishing in Surveillance & Society.

how much they are worried about it and do they change their behaviour accordingly. If one is concerned about privacy intrusion when online, it is actually about collecting the personal data and (mis)using personal information. Online privacy involves the rights of an individual concerning the storing, reusing and the provision of personal information to third parties, as well as displaying of information pertaining to oneself on the Internet. The invasion of privacy on the Internet includes the unauthorized collection, disclosure or other use of personal information (Wang, Lee, and Wang 1998).

We argue that Internet users' online privacy concerns in a post-transition country reflect citizens' surveillance concerns in post-communist society. We have conducted a large telephone survey in Croatia in 2016 on a nationally representative sample of more than 2000 Internet users in order to explore various aspects of citizens' attitudes towards surveillance and privacy in online environment. We explored the following research questions: Are there different groups of citizens that have different attitudes towards surveillance and privacy in online environment? Are there differences in behaviour among those groups? Are there differences in socio-demographic characteristics among those groups?

8.1. Data and methodology

The survey data employed originate from the large telephone survey we conducted in Croatia at the beginning of 2016. An online phone book was used as a sampling frame. The sample was created based on a one-way stratification by 21 counties. The sample allocated to each stratum was proportional to the assessed number of Internet users in each stratum. Within each stratum a 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 systematic sampling procedure. The final sample consists of 2,060 Internet users aged 18 or older. The summary statistics of sampled respondents is presented in Table 26.

The measurement instrument included 28 questions on online surveillance concern, trust in institutions, trust in people, perceived quality of regulation, perceived benefits of

Internet usage, fabrication of data, protection of data, and withholding data. Each item in the questionnaire was measured by a five-point Likert-type scale, ranging from 1 (strongly disagree, absolutely no) to 5 (strongly agree, absolutely yes).

Table 26. Summary statistics of sampled respondents, N=2,060

	%		%
Gender		2,501-5,000 HRK	14.8
Male	49.7	5,001-7,500 HRK	21.9
Female	50.3	7,501-10,000 HRK	29.2
Age		10,001-12,500 HRK	13.3
18-29	27.2	12,501-15,000 HRK	9.6
30-39	26.8	More than 15,000 HRK	8.8
40-49	22.8	Occupation	
50-59	16.8	Owner of the company/craft	2.0
60+	6.4	Manager/official	2.1
Education		Professional	29.9
Primary school	0.8	Technician/clerk	18.1
Secondary school	50.2	Worker	24.7
University and higher education	45.9	Retired	8.7
Master's degree/doctoral title	3.1	Student	8.7
Income		Unemployed	5.0
Up to 2,500 HRK	2.5	Other	0.7

Source: Survey and authors' calculations.

Online surveillance concern variable was measured by using the adapted construct indicating an individual's level of perceived harm or vulnerability when using the Internet (Malhotra et al., 2004). We posit that the level of surveillance concern is associated with social trust an individual Internet user has and with his/hers perceptions on the regulatory framework in place. Therefore we have included the variables of trust in the analysis. Two sets of questions were employed, one designed to estimate the extent of confidence in institutions and another measuring general trust in people (Naef and Schupp, 2009).

There is a general consensus in the literature that information concern corresponds to a

person's willingness to render personal information (Dinev and Hart, 2006), to transaction activity (Pavlou, Liang, and Xue, 2007) and government regulation (Milberg, Smith, and Burke, 2000). 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, that sufficient legal regulation is in place to protect their privacy, and have greater trust and confidence in these power-holders. There is also research that examined the impacts of regulation, legal and regulatory policies on online privacy concern (Lwin, Wirtz, and Williams, 2007). Past research indicates 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, and Peng (2002) showed that regulation is considered to be very important in protecting online privacy, while the study of Lwin, Wirtz, and Williams (2007) showed that the perceived effectiveness of regulatory policies and their enforcement reduces consumer online privacy concern. Based on the previous findings, the perceived quality of regulation is assumed to be related to the online surveillance concern as well.

As a result of their concern, Internet users might engage in various types of protective behaviour, particularly in situations if they perceive the potential threats in online transactions. Lwin, Wirtz, and Williams (2007) suggest that one might fabricate personal information (i.e. disguise identity through providing false information); adopt technology to protect personal information (i.e. use encryption, cookie-busters and anti-tracking software), and withhold from interacting with a Website (i.e. refuse to provide information or to patronise web sites). Milne, Rohm, and Bahl (2004) suggest that individuals engage in online identity theft protection behaviour that includes checking the security of online forms using separate e-mail accounts, rejection of cookies, reading privacy policies, encrypting their e-mails. Therefore, behavioural variables in terms of fabrication of data, protection of data, and withholding data are included in the analysis. We were also interested to see if, despite the surveillance concern, Internet users value the perceived benefits of online activities.

Demographic characteristics of the respondents – in our case Internet users – might explain the level of online privacy concern (e.g. Zhang et al., 2002; Hoy and Milne, 2010), so gender,

age, education, household income, and occupation have been included in the analysis of surveillance concern as well.

The collected data were first analysed in a descriptive manner to determine the public opinion on online surveillance concern, the perceived quality of privacy regulation, trust in institutions and trust in people. Cronbach's alpha coefficients were calculated to quantify the scale reliabilities. For the second step, exploratory factor analysis was used to identify the factors of personal sets of values. Then, K-means cluster analysis was employed to determine the segments of population with similar values, while differences in respondents' values between the groups were analysed using chi-square test.

8.2. Results and discussion

The initial set of 28 items was tested by using exploratory factor analysis in order to test construct validity of applied measurement scales. Principal components analysis was employed to extract the factors. The Kaiser-Guttman rule was used to determine the number of factors to extract. The exploratory factor analysis indicated eight distinct factors, explaining 66.4 percent of the total variance (Table 27).

Table 27. Exploratory factor analysis results, factor loadings

Items	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7	Factor 8
p7_1								0,77
p7_2				0.73				
p7_3				0.82				
p7_4				0.84				
p8_6								0.68
p8_7								0.57
p8_8					0.87			
p8_9					0.93			
p8_10					0.86			
p8_28	0.76							
p8_29	0.58							
p8_30	0.79							
p8_31	0.87							
p8_32	0.88							
p8_33	0.56							
p8_49							0.88	
p8_50							0.88	
p8_51							0.44	
p9_1						0.81		
p9_2						0.80		
p9_3						0.75		
p9_4			0.87					
p9_5			0.83					
p9_6			0.79					
p9_7		0.77						
p9_8		0.88						
p9_9		0.81						
p9_10		0.79						

Confirmatory factor analysis (CFA) was performed as an additional test of construct validity. The specified measurement model included eight uncorrelated factors with uncorrelated measurement errors. The goodness-of-fit index (GFI) and adjusted goodness-of-fit index (AGFI) were 0.92 and 0.90, respectively. The normed fit index (NFI), non-normed fit index (NNFI), comparative fit index (CFI), and RMSEA were 0.90, 0.90, 0.91, and 0.058, respectively.

Fit indices indicated a reasonable level of fit of the model (Hu and Bentler, 1999). The values of fit indices obtained from the eight-factor model represent a substantial improvement over the values obtained from the one-factor model. The results of confirmatory factor analysis indicated an acceptable level of convergent and discriminant validity, and unidimensionality (Table 28).

Table 28. Confirmatory factor analysis results and Cronbach's alpha coefficients (α)

Items	Factor loadings
α = 0.75	
p7_2	0.70*
p7_3	0.85*
p7_4	0.91*
α = 0.50	
p7_1	0.63*
p8_6	0.68*
p8_7	0.27*
α = 0.87	
p8_8	1.04*
p8_9	1.27*
p8_10	0.97*
α = 0.86	
p8_28	0.85*
p8_29	0.49*
p8_30	0.92*
p8_31	1.27*
p8_32	1.25*
p8_33	0.49*

Items	Factor loadings
α = 0.68	
p8_49	0.79*
p8_50	0.87*
p8_51	0.31*
α = 0.73	
p9_1	0.85*
p9_2	0.89*
p9_3	0.87*
α = 0.80	
p9_4	1.07*
p9_5	1.09*
p9_6	0.77*
α = 0.84	
p9_7	0.74*
p9_8	0.72*
p9_9	0.61*
p9_10	0.58*

Note: CFA fit indices: GFI = 0.92, AGFI = 0.90; NFI = 0.90; NNFI = 0.90; CFI = 0.91; RMSEA = 0.058;
* Factor loadings significant at $p < 0.01$ level

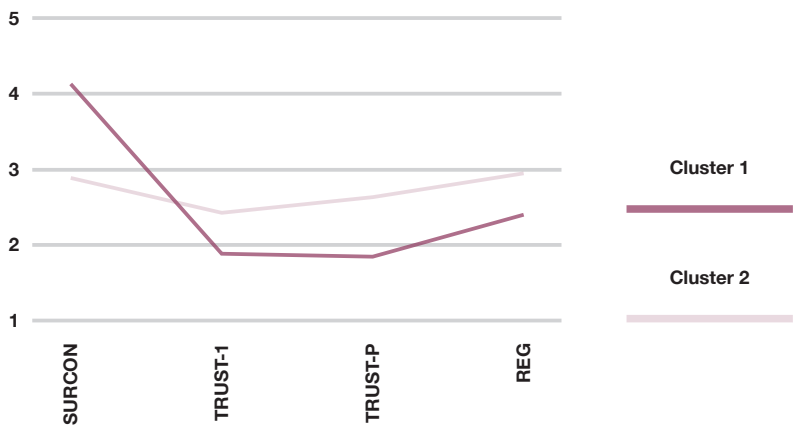
K-means cluster analysis was employed to classify Internet users in Croatia according to their online surveillance concern, the perceived quality of privacy regulation, trust in institutions and trust in people. The Hartigan index was used as a criterion for determining the number of clusters in a data set. Mean values were calculated for each factor as unweighted average values of corresponding items. These mean values were taken as an input in the K-means cluster analysis. The K-means cluster analysis indicated two homogeneous segments of citizens (Table 29).

The average mean values for the total sample show that Croatian Internet users are concerned about surveillance when online (mean = 3.56) and the perceptions of the quality of regulative is perceived low (mean = 2.29). They have almost no trust in other people and strangers. The trust in instructions is however, a bit stronger but still below mid-score of 3. The lack of social trust and in efficient regulative framework certainly contributes to the raising surveillance concern of Croatian citizens when online. Interestingly, there are two groups of Internet users in Croatia with statistically significant differences in all four analysed variables (Figure 9).

Table 29. Results of K-means cluster analysis

Variables	Acronym	Cluster 1 n=983	Cluster 2 n=1077	Sample Total n=2060	ANOVA
Surveillance concern	SURCON	4.28	2.90	3.56	F=2221.19; p=0.00
Trust in institutions	TRUST-I	1.93	2.39	2.75	F=215.76; p=0.00
Trust in people	TRUST-P	1.91	2.64	2.17	F=224.07; p=0.00
Perceived quality of regulation	REG	2.44	3.02	2.29	F=609.69; p=0.00

Figure 9. Surveillance-concern clusters of Internet users in Croatia



The first group, Cluster 1 (blue line) has higher levels of online surveillance concern, and at the same time this group has lower levels of trust in institutions, trust in people and perceived quality of privacy regulation. The second group, Cluster 2 (red line), has lower levels of online surveillance concern, but at the same time higher levels of trust in institutions, trust in people and perceived quality of privacy regulation.

T-tests and hi-squared tests were additionally conducted to explore differences among identified groups in behaviour and in socio-demographic characteristics (Table 30). Research results indicate that there are statistically significant differences among identified groups in all four analysed behavioural variables: engaging in protective behaviour (fabrication, protection and withholding), and giving out personal information on the Internet in exchange for benefits of Internet usage. The group of Internet users that are more concerned about surveillance are also more often engaged in all forms of protective behaviour, and are less likely to exchange their privacy for benefits of Internet usage. It is interesting to observe that an average Internet user in Croatia thinks that using the Internet offers some benefits (mean is slightly above 3). In order to protect their personal data when online, people prefer to withhold the information instead of installing protective software or fabricating the data (i.e. provide false date of birth).

Table 30. Differences in behaviour and demographics among clusters, ANOVA and chi-squared test results

Behavioural variables	Sample Total (n=2060)	Cluster 1 (n=983)	Cluster 2 (n=1077)	ANOVA
		Mean values		
Perceived benefits	2.92	2.76	3.07	F=39.03; p=0.00
Fabrication of data	2.10	2.18	2.03	F=11.36; p=0.00
Protection of data	1.81	1.91	1.71	F=18.63; p=0.00
Withholding data	4.52	4.63	4.41	F=48.55; p=0.00
Demographic variables				Chi-squared test
		Gender (%)		
Male	49.7	47.3	51.9	Pearson Chi-square: 4.35; p=0.00
Female	50.3	52.7	48.1	
		Age (%)		
18-29	27.2	24.3	29.9	Pearson Chi-square: 19.62; p=0.00
30-39	26.8	26.4	27.2	
40-49	22.8	22.5	23.1	
50-59	16.8	20.2	13.7	
60+	6.4	6.6	6.1	
		Education (%)		
Primary school	0.8	1.1	0.6	Pearson Chi-square: 25.17; p=0.00
Secondary school	50.2	55.4	45.5	
University and higher education	45.9	41.2	50.1	
Master degree /doctorate title	3.1	2.2	3.8	
		Income (%)		
Up to 2.500 HRK	2.5	2.8	2.2	Pearson Chi-square: 11.66; p=0.07
2.501-5.000 HRK	14.8	16.4	13.4	
5.001-7.500 HRK	21.9	22.2	21.6	
7.501-10.000 HRK	29.2	29.9	28.5	
10.001-12.500 HRK	13.3	13.1	13.5	
12.501-15.000 HRK	9.6	8.3	10.7	
More than 15.000 HRK	8.8	7.3	10.1	

Identified groups also differ in socio-demographic characteristics. Internet users from the group that is more concerned about online surveillance have on average lower level of education, and are older. Also, there are more females in this group. On the other hand,

Internet users from group that is less concerned about online surveillance have on average higher level of education, and are younger. There are more males in this group.

8.3. Conclusion

Empirical research on the large sample of Internet users in Croatia showed that there are clearly two groups of citizens sharing different levels of surveillance concern. More concerned Internet users have much lower social trust and perceive the quality of relevant regulation as poor. This group consists of mostly older citizens and predominantly with secondary education level or less, with lower household income. Surveillance concern results in more protective behaviour of Internet users in terms of giving false information on the Internet, sustaining from giving out personal information, etc. It leads us to conclude that surveillance concern in the online environment has behavioural consequences. More concerned people are older and have low trust in institutions and regulation, which corresponds to the previous negative experience originating from the socialist past of Croatia. As far as the older citizens are concerned, it seems that transition period did not erase individual surveillance memories that remained from the past. The results of this empirical research fill the gap in the underexplored area of communist past and contemporary online surveillance concern literature.

The findings of this research provide better understanding of surveillance concern among Internet users in a post-communist country and its interrelationships with behaviour and socio-demographics. The findings also provide an important prerequisite for better understanding of online behaviour, since surveillance concern stands as determinant of individual behaviour in online environm

9. EXTENDED MODEL OF ONLINE PRIVACY CONCERN[9]

Important parts of our living in the digital age are activities we all do when online. There is a raising interest in different aspects of this highly innovative environment and decision-making of Internet users, followed by an increased number of both theoretical and empirical studies on the privacy issues online. However, new research questions emerge. Confronted with the dilemma if there is any privacy when online, we are intrigued to know how much Internet users are nowadays aware or concerned about privacy intrusion. Do they change their behavior accordingly? What actions do they take when facing online privacy issues? Is privacy of a typical Internet user protected by regulations? Do we trust business privacy protection policy or national regulators? Finally, do people in different societal groups share similar attitudes about online privacy and would they take similar actions? If not, what factors explain the variations? These questions intrigued our research curiosity and stand in the core of this research.

Although previous studies have proposed various variables, concepts, and tested different theoretical models of antecedents and consequences of online privacy concern, there is no single widely accepted model of online privacy concern (Gurung and Jain, 2009). The extant body of research covering the online privacy theme deals with a limited number of antecedents and consequences, focusing on particular determinants, causes and consequences of either rather narrow or too general online privacy concern aspects. We have identified a lack of a comprehensive and integrated theoretical framework that would consolidate various streams of research into one model as a missing link in the literature in the online privacy concern field, and this research is meant to fill that gap.

The paper is structured as follows. In the next chapter we offer a brief literature of online privacy concern and an outline of the conceptual model of online privacy concern, its antecedents and consequences. Methodology applied to test the model of online privacy concern and

9 This 'master' paper has been presented at the 7th GIKA Conference in Lisabon, June 2017.

decision-making of Internet users in Croatia is described in the following chapter, including data collection, measures, survey questionnaire items, and methods to test the hypotheses. Results are discussed in the fourth chapter, and the last chapter concludes on findings and implications.

9.1. Literature review and conceptual model

With the spread of the Internet, more studies conceptualize and explore online privacy concern, which is considered to be a subset of consumer information privacy. In the digital era, the meaning of privacy has evolved and now focuses on personal information shared with family, friends, businesses, and strangers, while consumers must actively participate in self-protection as new digital technologies might be harmful for them (Markos, Labrecque, and Milne, 2012). Online privacy involves the rights of an individual concerning the storing, reusing, provision of personal information to third parties, and displaying of information pertaining to oneself on the Internet. The invasion of privacy on the Internet includes the unauthorized collection, disclosure or other use of personal information (Wang, Lee, and Wang 1998). The conceptualizations and measurement of online privacy concerns construct differ significantly across studies; however, the constructs of privacy concern share some common items and dimensions (Li, 2011).

Online privacy literature at the first place deals with the problem of how to measure privacy concern of Internet users. Based on their survey and analysis, Buchanan et al. (2007) suggested three scales for measuring the level of online privacy concern: one general called 'privacy concern' which is defined through people's attitude towards privacy, and two behavioral, 'general caution' and 'technical protection' which concern people's demeanor with regards to protection of their privacy.

Bearing in mind that privacy in an online context refers to "the rights and interests of an individual that apply to the processing of the information obtained from or about that individual" (Gellman and Dickson, 2011:268), and that advances in information technology (IT) pose multifaceted challenges to data usage and security (Nemati, 2011), we are led to

think of the cultural heritage that shapes our understanding of privacy rights and interests as well. The level of online privacy concern shapes our behavior on the Internet and beyond. Compared to the usage of traditional media in the past, consumers became more alert to information privacy issues when online (Kumar and Reinartz, 2012). Online privacy concern is expected to alter protective behavior of an Internet user who decides to withhold, fabricate or additionally protect his/hers information. The online privacy concern might influence adoption of new technologies, future usage of online services, and other types of behavior i.e. decision-making on, for example, sharing private information online. In developing the model we soon became aware that our model is not purely an economic research model but socio-economic one.

Gurung and Jain (2009) give broad literature overview of research on online privacy and propose an integrative framework of online privacy protection, including a non-exhaustive list of variables considered to be antecedents of online privacy protection behavior. We borrowed from the existing literature variables and approaches to build our conceptual model according to Smith, Dinev, and Xu (2011:1008) argument that “positivist privacy researchers should keep their eye on an optimized Antecedents -> Privacy Concern -> Outcomes macro model that eventually includes an expanded set of antecedents as well as an exhaustive set of outcomes”. Therefore, the central variable in our conceptual model is online privacy concern, where on the left side there is a list of determinants i.e. antecedents, and on the right side of the model are variables representing consequences of online privacy concern (Figure 1).

Online privacy concern reflects the level of concern felt by an individual when using the Internet. The intensity or range of online privacy concern is hard to measure and it is highly subjective. Actually our objective is to measure subjective notion of concern and here we have borrowed from the existing literature measurement scales and adapted them for an online environment starting from the Global Information Privacy Concern introduced by Smith, Milberg, and Burke (1996) and described in Malhotra, Kim, and Agarwal (2004).

Past research has identified a number of different antecedents to online privacy concerns, including user-level antecedents that are the focus of our research (see for example Graeff and Harmon, 2002; Dommeyer and Gross, 2003; Yao, Rice, and Wallis, 2007). In general, there are three broad categories of user-level antecedents: demographic factors (e.g. gender, education), experience factors (e.g. Internet use, web expertise) and socio-psychological factors (e.g. the psychological need for privacy, generalized self-efficacy, belief in privacy rights).

Implications of online privacy concern are listed on the right side of our model. These are consequences of online privacy concern divided into two groups: attitudes and behavior. Attitudes do not necessarily reflect behavior. The expected consequence of an increased online privacy concern is altered protective behavior in the form of withholding information, providing false information or protection of information including technical protection (e.g. software installed). Lwin et al. (2007) stated that reactive behavior implies personal information fabrication, withholding and protecting by using privacy enhancing technologies. Another behavioral reaction to an increased online privacy concern is less online usage in the future, including refraining from surfing on the Internet or limiting the range of online activities. People concerned about their privacy when online might change their intention to adopt new online services or technologies. More concerned users might decide not to make online purchases, or e-banking transactions. Some concerned people might refrain from social networks or even from using smartphones.

Our conceptual model was tested on the large dataset and using the methodology described in the next section.

9.2. Methodology

Data for this study were collected by Computer-Assisted Telephone Interviewing (CATI) method during a period of November 2015 to March 2016. Internet users in Croatia represent the population for this study, and secondary data were used (Stilus Media) to assess the number of Internet users in Croatia. Online phone book was used as a sampling frame. The

sample was made on a one-way stratification by 21 counties. The sample allocated to each stratum was proportional to the assessed number of Internet users each stratum. Within each stratum a combination of random and systematic sampling was applied. Pages from phone book were selected using simple random sampling procedure. Sample units within each page were selected applying systematic sampling procedure. The final sample consists of 2,060 Internet users aged 18 or older. The summary statistics of sampled respondents is presented in Table 31.

Table 31. Sample characteristics, N=2,060

Variable	%	Variable	%
Education groups		Manager/official	2.1
primary school or less	0.8	Professional	29.9
secondary education	50.2	Technician/clerk	18.1
tertiary educ./high school, university	45.9	Worker	24.7
master degree/doctoral title	3.1	Retired	8.7
Gender		Student	8.7
Female	50.3	Unemployed	5.0
Male	49.7	Other	0.7
Age groups		Income groups	
18 - 29	27.2	up to 2,500 HRK	2.5
30 - 39	26.8	2,501-5,000 HRK	14.8
40 - 49	22.8	5,001-7,500 HRK	21.9
50 - 59	16.8	7,501-10,000 HRK	29.2
60+	6.4	10,001-12,500 HRK	13.3
Occupation groups		12,501-15,000 HRK	9.6
Owner of the company / craft	2.0	more than 15,000 HRK	8.8
		Note: 1EUR= 7.5HRK (Croatian kuna). www.hnb.hr	

The questionnaire included items for all variables in our model (Figure 10). Traditional values variable (TRAD_VAL) was measured by single item developed by Lindeman and Verkasalo (2005) as part of their shortened version of Schwartz's value survey. Social trust (ST) items were taken from Naef and Schupp (2009) and they include two sets of items, one for measuring the trust in institutions and another measuring general trust in people. Perceived

quality of regulatory framework (REG) variable was measured by three items. Respondents were asked to declare if the existing country legislation and government effort is sufficient to protect online privacy or if there should be more strict regulation put in place to protect personal privacy online (Wirtz, Lwin, and Williams, 2007). Belief in privacy rights or need for privacy (NFP) scale was adopted from Yao, Rice, and Wallis (2007) and consists of three-items.

Computer anxiety variable (CA) was measured using the adapted items of Parasuraman and Igbaria (1990). Online privacy concern (OPC) items were taken from Smith, Milberg, and Burke (1996) covering various aspects of personal online privacy concern. Intention to share personal information online (SH) was measured by asking about the different types of information at different sharing platforms such as social networks. Respondents were asked if they put private information on the Internet, share private pictures, post their current location or company, and finally if they provide the credit card number when buying online. Items for variable Intention to adopt new technologies (NEWT) were taken from Wang, Dacko, and Gad (2008). Perceived benefits of using the Internet (BNF) variable was measured using the adapted items from Dinev and Hart (2006) and Malhotra, Kim, and Agarwal (2004). Respondents were also asked about trading off the potential privacy violations risks in the sake of personal interest to get information or services online. Protective behavior, which consists of fabrication of personal information (PB_FAB), sustaining from giving out personal information (PB_SUST) and using tools for actively protecting one's privacy (PB_PROT) is adopted from Wirtz, Lwin, and Williams (2007). Demographic characteristics of individual respondents were captured at the end of the questionnaire, and they included gender, age, education, and net monthly household income.

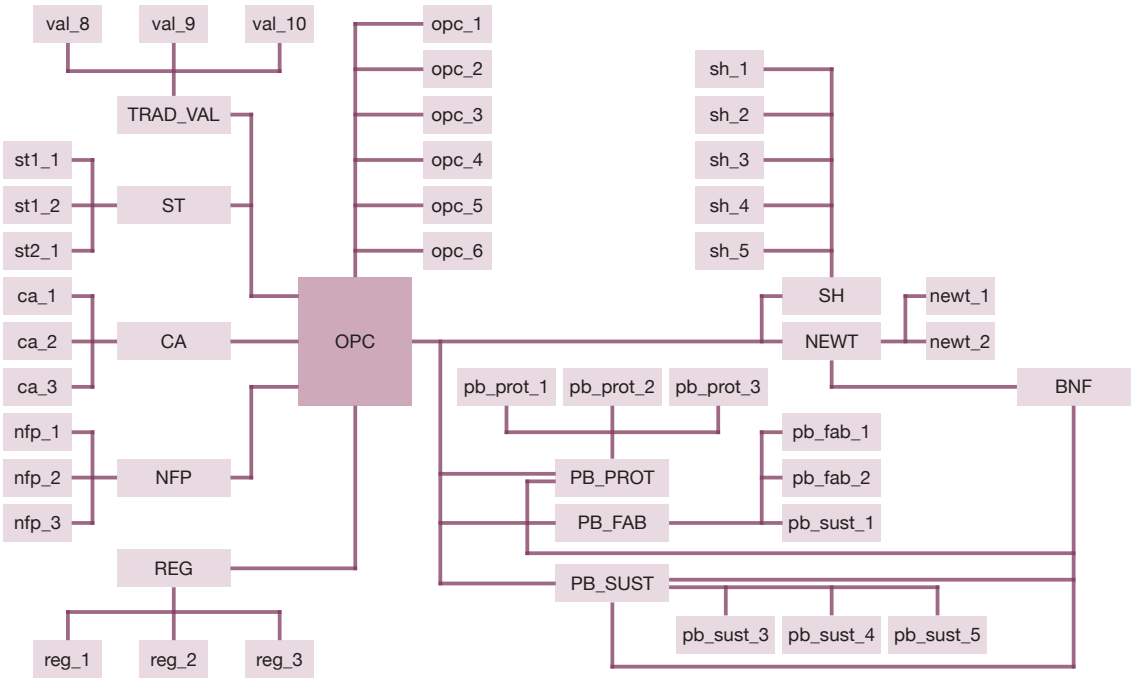
Structural model of online privacy concern and research hypotheses were tested using the SEM-PLS methodological approach[10]. Complete analysis was performed using the plspm package in R (Sanchez, Trinchera, and Russolillo, 2015).

10 Advantages of Partial Least Square usage for parameter estimation in structural equasion model is explained in Fornell and Bookstein (1982).

9.3. Results and discussion

Structural model of online privacy that is tested in this research is presented in Figure 10. Rectangles represent manifest variables (i.e. indicators – questions from the survey), while ellipses represent latent variables. Single headed arrows represent the causal relationship between latent variables. All variables are measured reflectively. Following Sanchez (2013) and Hair et al. (2014), we proceed with evaluation of estimated SEM-PLS model first by evaluating measurement and then the structural model.

Figure 10. Extended model of online privacy concern



The first criterion is internal consistency reliability. Based on the rule of thumb provided by Hair et al. (2014) and Sanchez (2013) on all measures of unidimensionality, it seems that the measurement model is well specified. Cronbach's alpha for all latent variables (except ST, NFP and REG) is above the threshold value of 0.7 provided by Sanchez (2013). According to Hair et al. (2014) the values of 0.6 are acceptable for exploratory research. This leaves

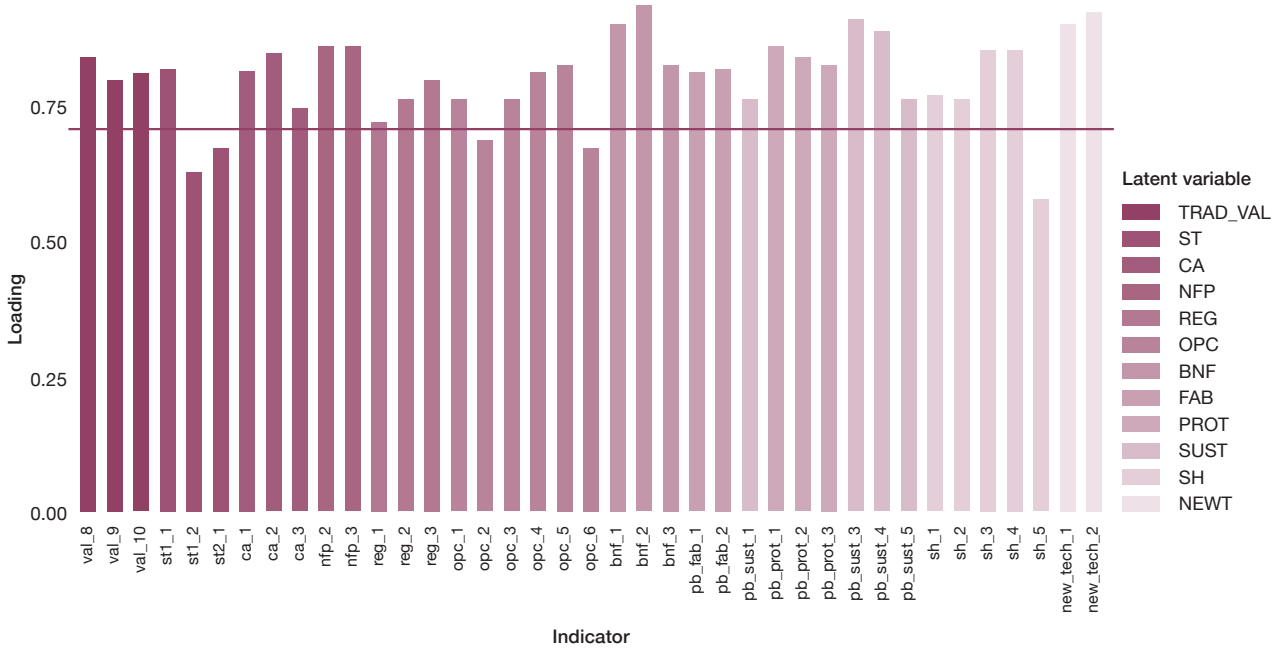
only ST as potentially problematic with regards to reliability. However, Diller-Goldstein's ρ, which is considered to be a better indicator than the Cronbach's alpha because it takes into account the extent to which the latent variable explains its block of indicators (Sanchez, 2013), is above the rule of thumb threshold value of 0.7 for all latent variables. This is also supported by the eigenvalues, with first eigenvalues of all variables being significantly above 1, and second eigenvalues below 1.

Next, we examined the convergent validity, which is the extent to which a measure correlates positively with alternative measures of the same construct (Hair et al., 2014: 102). To establish convergent validity, we considered the outer loadings of indicators and average variance extracted (AVE). Outer loadings are plotted in Figure 11. Loadings of 0.7 and above are considered acceptable since this means that the latent variable explains a large part of that indicators variance, at least 50 percent. Five indicators are below this threshold value. However, in line with the suggestions from Hair et al. (2014), items with loadings between 0.4 and 0.7 should be considered for removal from the scale only if deleting the indicator leads to the increase in the composite reliability, measured by AVE. Removing the two items from OPC construct leads to increase in AVE from 0.57 to 0.73. Removing one item from SH construct leads also to a large increase from 0.58 to 0.71. These items are therefore removed from the further analysis. Considering the ST construct – two out of three items have loadings below threshold. Deleting both items would lead to one item scale which is strongly advised against. We opt for the middle approach and deleting only item with the lowest loading which increases AVE from 0.5 to 0.67.

Next, we examined the discriminant validity of the measurement model, or, the extent to which a construct is truly distinct from other constructs by empirical standards (Hair et al., 2014). By looking at the cross loadings we found that all indicators' outer loadings on the associated constructs are larger than all their loadings on other constructs. Therefore, discriminant validity is established. More conservative approach for establishing discriminant validity is the Fornell-Larcker criterion (Hair et al., 2014). This criterion compares the square root of AVE with correlations between latent variables. To establish discriminant validity, the

square root of AVE should be larger than the largest correlation with any other construct and by this criterion discriminant validity is also established.

Figure 11. Chart of outer loadings



Source: author's calculations

Now we proceed with the assessment of structural model results. Goodness-of-Fit (GoF) measures usual for CB-SEM, such as chi-square statistics or the various fit indices, are not applicable in SEM-PLS context (Hair et al., 2014). Tenenhaus et al. (2005) propose global GoF index for validating the PLS model globally. However, Henseler, and Sarstedt (2013) provide evidence from simulation that the proposed GoF index is not suitable for model validation. The effect size measures how much the coefficient of determination changes when exogenous construct is excluded from the model, or formally[11]:

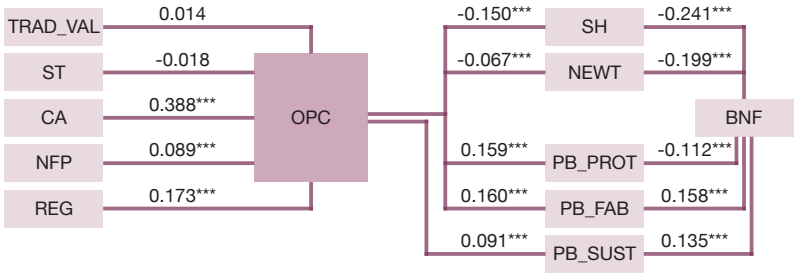
$$f^2 = \frac{R^2_{\text{excluded}} - R^2_{\text{included}}}{1 - R^2_{\text{excluded}}}$$

From exogenous variables in the model, only computer anxiety has moderate effect on online privacy concern (=0.18), while other variables have small effect according to Cohen

11 For more details see Hair et al., 2014.

(1988) with between 0 and 0.06. Standardized coefficients of the structural model are given in Figure 12.

Figure 12. Path coefficients of the structural model



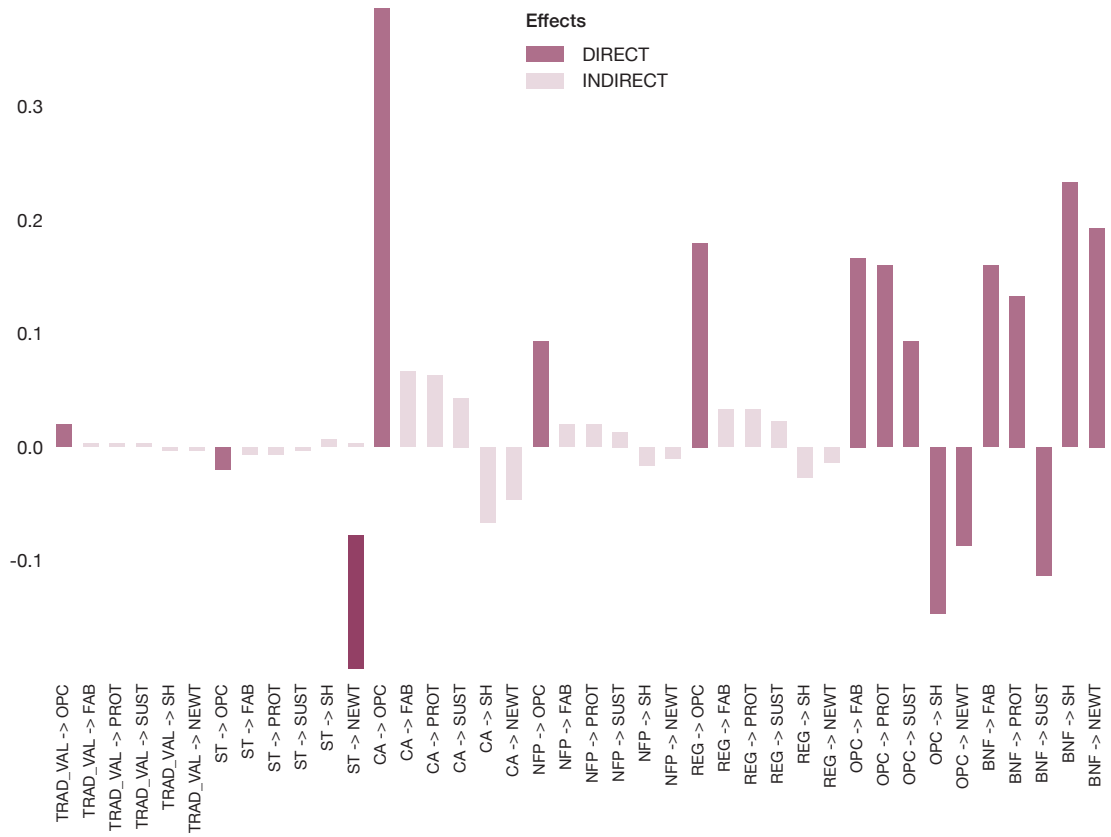
Note: *** significant at 1 percent level

Traditional values and social trust do not have significant impact on online privacy concern. It means that Internet users who care about family ties, loyalty, respect to authorities and similar traditional values, regardless of those characteristics might be more or less concerned for their privacy when online. The same stands for social trust which, although seems to be negatively associated with online privacy concern, is not significant. It indicates that no matter how low the trust in other people or institutions might be, the online privacy concern is determined by other factors. Among them, the highest influence has been observed in the level of computer anxiety. Internet users who feel insecure and might be even afraid of unknown 'superpowers' of computers and of IT in general, feel as well that their privacy online might be threatened. Significant increase in online privacy concern is due to the lack of believe in the efficacy of regulatory framework and policies in place. This goes hand in hand with personal awareness of privacy rights: the stronger the belief that one has right to enjoy privacy, the more concerned about privacy online an Internet user is.

The rest of path coefficients are all significant. On the consequences side of the model, there is a strong and significant positive relation between online privacy concern and protective behavior. As expected, more concerned Internet users will decide to take actions that will protect them from the privacy intrusion. These actions range from active protection,

fabrication and sharing of personal information on the Internet. As far as it considers Internet users intentions, the analysis confirmed that they would change their intentions to share personal information and intentions to adopt new technologies. More privacy concerned Internet users decide to act more prudently when online. One should note however that not all coefficients are substantial. Moreover, it seems that, on average, perceived benefits of using the Internet outweighs potential associated costs with privacy concern of people. for endogenous latent variables are as follows: OPC = 0.23, FAB = 0.05, PROT = 0.04, SUST = 0.02, SH = 0.09, and NEWT = 0.05. As Hair et al. (2014) note, values of 0.2 are considered high in some disciplines, such as consumer behavior. Other endogenous variables seem not to be predominantly explained by their antecedents in the model. Figure 13 plots direct effects from Figure 12, as well as indirect effects.

Figure 13. Direct and indirect effects in the structural model



As expected, computer anxiety, the most substantial antecedent of online privacy concern, also has the largest indirect effects on consequences of online privacy concern. Other indirect effects in the model are irrelevant by their size.

9.4. Conclusion

Among variables included in the model as antecedents, traditional personal values and social trust of Internet users do not have a significant impact on online privacy concern. Computer anxiety seems to have the largest impact on level of online privacy concern, followed by perceived quality of the regulatory framework and then by respondents' belief in privacy rights. On the other side of the model, online privacy concern has the largest impact on active protection, fabrication and sharing of personal information on the Internet. Moreover, perceived benefits of using the Internet outweigh potential associated costs with privacy concern of people when online. This research developed comprehensive and integrated model of antecedents and consequences of online privacy concern, and filling that gap stands as a main contribution of this work.

As the level of online privacy concern shapes our behavior on the Internet and beyond, the findings on individual-user level might contribute to further advance academic research, in particular in the field of economics. Besides that, this research unveils the trade-off between privacy concern and perceived benefits of using the Internet. The online privacy concern might influence adoption of new technologies, future usage of online services, and other types of behavior. Therefore, these findings may be useful for practitioners as well, notably in helping companies to develop business strategies and regulators to frame privacy policy better.

10. PRIVACY ISSUES IN THE COMMERCIAL SETTING

In contrast to the general privacy domain, from the economic point of view, online privacy concern is closely related to the privacy concern in commercial setting[12]. There are two reasons to study past research related to this issue. The first reason is that most of privacy-related research is driven by the need to develop efficient marketing strategies of the companies and studying these relations might help us build the "Extended general model of online privacy concern". Our intuition is that some consumer privacy patterns might apply to general online behaviour, so past research in the consumer privacy domain is instructive for PRICON. The second reason is that we borrowed some items (from the past research) for generating general PRICON survey. Consumer online privacy concern literature section gives additional insights into privacy issues and extends the general online privacy concern literature review.

Previous studies indicate that the Internet and associated digital communication technologies have changed people's lives and business practices significantly (Reed, 2014). The expanding adoption of the Internet and the increasing number of Internet users provides the basis for the development of online businesses. Nowadays, the Internet has become an important marketing tool, while the intelligent use of consumer data is considered to be an important competitive advantage of companies (Krohn, Luo, and Hsu, 2002; Beveridge, Cook, and Stubbings, 2015). However, increased volume of personal information gathered from individuals in online commercial transactions, its manipulation and trade, and resulting intensified online marketing communications have increased a consumer concern about online privacy.

In the e-commerce literature, research has focused on online information privacy concern from the consumer perspective (Li, 2014). Although various antecedents and consequences

12 This chapter is based on published work: Anić, Ivan-Damir: The development of database marketing: does consumer information privacy matter?. // Zbornik radova Ekonomskog fakulteta Sveučilišta u Mostaru. 21 (2015) ; 39-56 (review article).

of online privacy concern were identified in the past research, no consensus has been reached on their relations with privacy concern. Privacy has been shown to be important to many consumers, and it might negatively affect consumer willingness to provide personal information, the usage of Internet, and their purchases of goods and services over the Internet (Malhotra, Kim, and Agarwal, 2004; Nam et al., 2006). The loss of consumer data has been seen as a real threat to modern businesses (Beveridge, Cook, and Stubbings, 2015), and therefore, reducing online privacy concern and increasing consumer confidence in using the Internet is the key to success of digital marketing and e-commerce (Nam et al., 2006; Beveridge, Cook, and Stubbings, 2015).

In this chapter we explore the concept and major issues related to online privacy concern, its antecedents and consequences. This chapter is focused on the following research questions: (1) In what situations online consumer privacy matters? (2) What are major factors that affect online privacy concern? (3) What are major consequences of online privacy concern? (4) What approaches can be used to reduce privacy concern? A comprehensive literature review is conducted to examine those issues, which are important to the development of knowledge in this field. The chapter is focused on the analysis of privacy concern from consumer perspective in the Internet and e-commerce environment. A brief overview of digital marketing issues is also provided in this chapter.

Understanding consumer online privacy concern might help companies to develop more affective digital marketing strategies in order to increase the likelihood of consumers to take more proactive approach to online marketing initiatives and increase purchases over the Internet.

The second section of this chapter presents the literature review on the concept of consumer online privacy concern. In the third section, risks and issues related to online privacy concern in commercial setting are described, while the fourth section contains the identification of major antecedents and consequences of consumer online privacy concern. The chapter concludes with the conclusion and managerial implications of consumer online privacy concern.

10.1. Risks and issues related to online privacy concern in commercial setting

Developing consumers databases from information obtained in online transactions has become particularly important for companies. Such information is collected for example from individuals who register and shop online that use credit cards or just surf on the Internet. The information about individuals and their pattern of behaviour is collected all over the Internet by popular services. Many e-commerce sites directly ask users for personal information through forms, or they might record data about their users' browsing habits[13]. Marketers rely on third-party sources of data as a source of consumer data.

By using consumer databases, companies might develop detailed demographic profiles of Internet users, identify most valuable customers, identify new market trends, create advertising strategies for customer acquisition and retention, and send tailored messages and recommendations to their customers based on their preferences and locations (Kosinski, Stillwell, and Graepel, 2013; SAS, Wikipedia). Companies might also reduce marketing expenses, decrease the costs of communication and marketing expenses, and optimise their product prices (Hui and Png, 2006).

Various surveys indicate that the majority of marketers and consumers are generally positive about the usage of Internet, but they seem to be concerned about the online privacy. In the EU, 74% of citizens see disclosing personal information as a part of modern life, while 70% of respondents were concerned that their personal data held by companies may be misused (European Commission, 2011). Consumers' concern about their privacy originates from a lack of knowledge about how their data is used by marketers and the opinion that disclosing information may make them vulnerable to threats to identity and personal safety (Milne, Rohm, and Bahl, 2004).

13 E-commerce is World Wide Web-based buying and selling of goods and services, and it includes electronic data interchange in conducting transactions among suppliers and customers.

The following biggest online privacy threats have been identified in marketing research studies: cookie proliferation (as advertisers and marketers seek to learn more about their consumers and their purchasing patterns), seizing cloud data (as advertisers and marketers try to use this data as a source of information), and location data betrayal (with knowing consumer locations advertisers and marketers might send their consumers promotions for nearby businesses, wherever they are close on this locations) (PCWorld, 2013). Some web-based companies might also even sell consumer information to third parties, and expose their customers to further privacy intrusion. Some other potential Internet privacy risks have been identified in online transactions: malware, spyware, web bug, phishing, parking, social engineering, malicious proxy server, use of weak passwords, using the same login name and/or password for multiple accounts, where one compromised account leads to other accounts being compromised, allowing unused or little used accounts, where unauthorised use is likely to go unnoticed, to remain active, using out-of-date software that may contain vulnerabilities that have been fixed in newer more up-to-date versions, WebRTC protocol which suffers from serious security flaws. All those threats might be very harmful for the safety of individuals.

As a consequence, consumers might want to protect their privacy and safety in online transactions. Consumers might become hesitant to disclose their personal information to marketers, or to conduct monetary transactions over the web and online purchases (Thomas and Maurer, 1997; Bansal, Zahedi, and Gefen, 2016). Individuals with high privacy concern would be more likely to minimise their vulnerability by limiting Internet activity (Dinev and Hart, 2004). Therefore, reducing privacy concern and increasing consumer confidence in using Internet has become the primary goal of marketers (Nam et al., 2006).

10.2. Antecedents to online privacy concern in commercial setting

Various antecedent factors to online privacy concern were analysed and proposed in previous research, and yet the results are mixed for certain factors (Li, 2011). The most examined and influential antecedents are the following:

- Demographic variables,
- Personality traits,
- Perceived ability to control information,
- Internet users' knowledge and experience,
- Company and Website-related factors (e.g.. established privacy policies, company reputation, specific attributes provided by a website)
- Information contingencies (e.g. type of information and information sensitivity).

Demographic variables (i.e. age, gender, education and income) have been the most frequently analysed antecedents of privacy concern. Previous research shows that women are more concerned about privacy and the protection of their personal information on the Internet than men (Sheehan, 1999; O'Neil, 2001; Graeff and Harmon, 2002; Mathiyalakan et al., 2014), although there are studies suggesting that females and males might be equally concerned about privacy in on-line transactions (Zhang, Chen, and Lee, 2013). When compared to men, women are more likely to be the victims of online abuse, and thus they might engage in privacy protection behaviour (Hoy and Milne, 2010). On the other hand, male consumers are more willing to take risks and feel more comfortable making purchases on the Internet (Sheehan, 1999; Graeffand Harmon 2002; Fogel and Nehmad, 2009; Zhang, Chen, and Lee, 2013). Men have stronger interest in computers and computer skills and are more likely to take active control (Chen and Rea, 2004). Age was shown to be positively related to online privacy concern, which means that older individuals are more concerned about privacy than younger ones (Graeff and Harmon, 2002; Milne et al., 2012). Older consumers are less comfortable making credit card purchases on the Internet (Graeff and Harmon, 2002). Many studies further indicate that higher income consumers are less concerned about their privacy than low income consumers (Milne and Boza, 1999; Graeff and Harmon, 2002; O'Neil, 2001). There are studies that suggest that education is positively correlated with privacy concern (Zhang, Chen, and Lee, 2013), although some studies suggest an absence or negative relationship (Milne, Beckman, and Taubman, 1996).

There are many studies that explored and conceptualised consumer concern for information

privacy that can be defined as consumer concern for personal information. Concern for Information Privacy (CFIP) is considered to be the most important factor affecting the development of consumer databases. CFIP deals with the rights of those people whose information is shared and arises whenever users suspect that their personal information rights might be violated (Wang, Lee, and Wang 1998). Smith, Milberg, and Burke (1996) developed a 15-item scale that measures CFIP and includes four dimensions: improper access to personal information, collection of personal information, errors in personal information, and unauthorised secondary use of personal information. This scale has been tested in several studies and environments (Milberg, Smith, and Burke 2000; Okazaki, Li, and Hirose, 2009).

Various personality traits were examined in past research, including the impact of paranoia, social criticism, cynical distrust, social awareness, conscientiousness, openness to experience (all having positive relationships with privacy concern), and agreeableness (negative impact on privacy concern) (Li, 2011). Yao, Rice, and Wallis (2007) suggest that the need for privacy also affects online privacy concern, while Stewart and Segars (2002) found that there is a positive relationship between computer anxiety and CFIP, where computer anxiety includes the tendency of individuals to be uneasy, apprehensive, or fearful about the current or future use of computers (Li, 2011). The perceived ability to control the data was also shown to be an antecedent of privacy concern, in such a way that privacy concern is likely to be reduced if the level of ability to control information collection and dissemination increases (Milne and Boza, 1999; Bandyopadhyay, 2011). Consumers tend to think that information disclosure is less invasive to their privacy, and less likely to lead to negative consequences, when they believe that they can control their information.

Previous studies show that privacy concerns might vary based on person's knowledge and experience. A few studies suggest that increased Internet users' experience in conducting Internet-related activities may be negatively correlated with their concern about privacy (Metzger, 2004). Increased familiarity should reduce the anxiety and increase the usage of new technologies. The more people engage in diverse online activities and the greater fluency they have in Internet and Web activities, the better understanding they have about

advantages and potential threats associated with these activities (Rice, 2006). However, the study of Yao, Rice, and Wallis (2007) did not confirm the hypotheses that Internet use diversity and fluency directly affect online privacy experience. In fact, the need for privacy positively affects beliefs in privacy rights, which increases concern about privacy, while Internet use diversity affects positively Internet use fluency, which affects beliefs in privacy rights. This can be explained by the fact that an increase in Internet use diversity and fluency may lead to a general sense of control over potential threats to online privacy, but also may increase the exposure to more threats, and thus the concern about online privacy may not decrease for experienced users. As users gain more knowledge about Internet- privacy-related issues, they may become aware of online privacy threats, while a novice user may be worried about online transactions to a great extent (Yao, Rice, and Wallis, 2007). The impact of time consumers spend online on privacy should also be complex, meaning that the more time consumers spend online, the more knowledgeable they might become, which may decrease their privacy concern. However, the more knowledge they accumulate, they might become more aware of potential Internet threats and thus become more privacy concerned.

Past studies provide strong empirical support that Internet privacy risks and prior negative online experience negatively affect consumer online privacy concern, in such way that the more consumers have had previous negative experiences on the Internet, the more concerned they are about their privacy (Okazaki, Li, and Hirose, 2009). A single event that induces a negative experience can increase privacy concern, even if users have mostly positive experiences (Okazaki, Li, and Hirose, 2009). Previous negative experience weakens consumer trust and increases perceived risk and might increase individual's tendency to protect their behaviour on the Internet (Cho and Cheon, 2004).

Privacy concern was also shown to be influenced by organisational factors. Firm reputation can increase the trust and perceptions of a customer-company relationship (Schoenbachler and Gordon, 2002). Consumers may be more accepting of potential privacy infringements when they are conducted by certain kinds of companies, such as those with whom consumers are already familiar, or who supply products that appear to be potentially useful (Wang and

Petrison, 1993). Third-party seal assurance (e.g. TRUSTe and BBB9) might also reduce online privacy concern (Miyazaki and Krishnamurthy, 2002; Nam et al., 2006).

Privacy concern about a website is a type of situation-specific concern that deals with the privacy perceptions about a specific website, and occurs when the actual privacy on the website does not match the expected privacy (Li, 2014). Several factors were found to affect website privacy concern, including the reputation of a website, privacy policy and rewards, privacy assurance, information sensitivity, website informativeness, perceived privacy control and privacy risk (Li, 2014). Privacy concern was also shown to be negatively associated with consumer attitudes towards the website comfort, satisfaction and likeness of surfing the web, building relationships with companies, service provided online and future intent of using the website (Krohn, Luo, and Hsu, 2002). Positive consumer perceptions of the e-tailer privacy policy were shown to have negative influence on their privacy concerns (Kiryanova and Makienko, 2011). If companies establish and enforce privacy policies and increase website informativeness, they can also reduce privacy concern (Pavlou, Liang, and Xue, 2007; Li, 2011). The respondent's trust in the website and perceived risk were found to predict their willingness to disclose personal information (Heirman et al., 2013).

Another stream of research indicates that the type of information requested and information sensitivity affect privacy concern (Li, 2011). Malhotra, Kim and Agarwal (2004) found that a request for more sensitive information in an e-commerce setting reduces trust and increases perceived risk, because the request makes consumers more cautious and suspicious about a marketer (Okazaki, Li, and Hirose, 2009). Consumers are most willing to provide marketers with demographic and lifestyle information, while they are the least willing to provide financial information and personal identifiers, like annual household income, credit card information, telephone and social security numbers (Phelps, Nowak, and Ferrell, 2000; Milne et al., 2012). The study of Lwin, Wirtz, and Williams (2007) indicates that a strong business policy is effective in reducing concern when low sensitivity data are gathered, but insufficient in reducing concern for highly sensitive data. When sensitive data are collected that are not related to the business context, privacy concern is likely to increase.

10.3. Consequences of online privacy concern in commercial setting

Past research has identified various consequences of online privacy concern. Some of the most important variables are the following:

- Protective behaviour,
- Behavioural intentions (e.g. purchase intentions),
- Actual behaviour (e.g. actual consumer purchases),
- Willingness to provide personal information (in online transactions for developing consumer databases),
- Degree of regulatory control.

As a result of privacy concern, consumers might engage in various types of protective behaviour, particularly in situations when they perceive the potential threats in online transactions. Privacy concern has a significant impact on individuals' beliefs about information risk, behavioural intention to provide information and actual behaviours (Li, 2011). Lwin, Wirtz, and Williams (2007) suggest that consumers might fabricate personal information (i.e. disguise identity through providing false information); adopt technology to protect personal information (i.e. use encryption, cookie-busters and anti-tracking software), and withhold from interacting with a Website (i.e. refuse to provide information or to patronise web sites). The study of Sheehan and Hoy (1999) showed that as individuals' concern increase, they are likely to increase the frequency with which they provide incomplete information to websites, the frequency with which they contact an Internet Service Provider about unsolicited e-mail, the frequency with which they send a highly negative message to those sending unsolicited e-mail, the frequency with which they request their names be removed from mailing lists, while they might decrease the frequency with which they register for a web site. Milne, Rohm, and Bahl (2004) suggest that individuals engage in online identity theft protection behaviour that includes checking the security of online forms using separate e-mail accounts,

rejection of cookies, reading privacy policies, encrypting their e-mails. Son and Kim (2008) showed that (except for misrepresentation) privacy concern has positive impact on refusal to provide information, removal of information, negative word-of-mouth, complaining to the company, and complaining to third parties. The study by Zviran (2008) showed that privacy concern was positively associated with refraining from surfing, cancelling online spending and reducing volume of online spending. Previous studies also suggest that consumers who are concerned about their online privacy will be unwilling to disclose personal information in online transactions (Nam et al., 2006; Faja and Trimi, 2006; Dinev and Hart, 2006). This may result in, e.g. browsing Websites where no personal data is captured, or providing only limited and anonymous, or even false personal information to Websites (Dinev and Hart, 2006) that require registration to use content (Bandyopadhyay, 2009).

Privacy concern was shown to significantly affect consumer intentions and actual online behaviour (Li, 2011). Empirical evidence indicates that concerns for privacy might negatively affect purchase intentions (Phelps, Nowak, and Ferrell, 2000; Phelps, D'Souza, and Nowak, 2001; Eastlick, Lotz, and Warrington, 2006), the willingness to buy (Faja and Trimi, 2006), and the intention to transact (Dinev and Hart, 2006). Furthermore, consumer privacy concerns negatively affect direct marketing usage (Milne and Boza, 1999), online transactions (Akhter, 2014), and consumer purchases (Phelps, D'Souza, and Nowak, 2001; Krohn, Luo, and Hsu, 2002). Consumers highly concerned about their privacy exhibited lower recency, frequency and monetary value of catalog purchases (Phelps, D'Souza, and Nowak, 2001). Privacy concern was also shown to be negatively related with e-commerce use (Dinev et al., 2006). It has also a negative impact on intention to adopt personalised services (Sheng, Nah, and Siau, 2008).

There is also research that examined the impacts of regulation, legal and regulatory policies on online privacy concern (Lwin, Wirtz, and Williams, 2007). Past research indicates 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, and Peng (2002) showed that regulation is considered to be very important in protecting online privacy, while the

study of Lwin, Wirtz, and Williams (2007) showed that perceived effectiveness of regulatory policies and their enforcement reduces consumer online privacy concern.

10.4. Various approaches to solving consumer privacy concerns

Past research indicates that consumers require both company policies and governmental regulations to safeguard their online privacy (Lwin, Wirtz, and Williams, 2007). Privacy regulations vary depending on both philosophical and jurisdictional considerations, from countries that have no regulations to those with strict and formal laws (De Pechpeyrou and Nicholson, 2012). At the low-government involvement (e.g. the US), the government allows corporations to monitor themselves through self-regulation principles, while at the high-government involvement (e.g. Sweden), the authorities regulate all corporate use of personal data, including the right to conduct inspections within corporations (De Pechpeyrou and Nicholson, 2012). In the US, there is a variety of state and federal laws which regulate the gathering and use of credit data, the gathering and use of consumer health data, and various programs that enable consumers to suppress their telephones numbers from telemarketing. In the EU, the Digital Agenda of European Union is one of the seven pillars of the Europe 2020 Strategy which sets objectives for the growth of the EU by 2020, while trust, privacy and security on the Internet are seen as vital drivers of the growth of digital economy (European Commission, 2013). The European Commission has established a set of data protection rules that determine what uses can be made of customer data and how consumers can influence what data are retained. The European Union requires all member states to legislate to ensure that citizens have a right to privacy.

Several researchers have proposed various ways to decrease high levels of consumer privacy concern from company perspective. Phelps, Nowak, and Ferrell (2000) suggest that privacy concerns can be reduced by providing consumers with more control over the initial gathering and subsequent dissemination of personal information (Dolnicar and Jordaan, 2007). For companies, it is important to develop trust through operational demonstrations that they are competent, serious and that they fulfil their promises. Companies might provide

more information on when information is collected, how it will be used, and who will have access to the data. They should ensure that corporate policy on privacy is communicated in comprehensive privacy notices that are highly visible on their Websites. Businesses should communicate why information is needed and how it will be relevant to their business, and how information disclosure might benefit consumers (Lwin, Wirtz, and Williams, 2007). Finally, Internet users should also protect themselves by updating virus protection, using security settings, downloading patches, installing a firewall, screening e-mail, shutting down spyware, controlling cookies, using encryption, fending off browser hijackers, and blocking pop-ups (Mediati, 2010).

Past research indicates that the Internet, associated digital communication technologies and the application of digital marketing are expanding very fast. New digital technology offers companies a number of opportunities in the field of consumer data collection, its analysis, market segmentation, online advertising, product offering and online sales. However, the volume of data collection and manipulation with consumer personal data, the intensity of advertising campaigns accompanied by a growing number of potential threats on the Internet for the identity and the safety of an individual, raise the issues related to online privacy concern in commercial transactions.

Past research shows that there is no universally accepted definition of online privacy concern and various concepts and measures exist. Despite this, online privacy concern contains some common items and dimensions. Various antecedents of online privacy concern and its consequences were analysed and proposed in previous research, while the results are mixed and much uncertainty still exists, especially in underdeveloped post-transition economies.

The most examined and influential antecedents are demographic variables, personality traits, perceived ability to control information, internet users' knowledge and experience, company-related factors and information contingencies. As a result of privacy concern, consumers might engage in various types of protective behaviour, particularly in situations when they perceive the existence of potential threats in online transactions. Empirical evidence indicates

that concern for privacy might negatively affect purchase intentions, the willingness to buy, the intention to transact, future direct marketing usage and consumer purchases. Privacy concern was also shown to be negatively related with e-commerce use and has a negative impact on intention to adopt personalised services. Past research shows that regulation is considered to be very important in protecting online privacy.

Literature review presented in this chapter strongly highlights the importance of online privacy concerns, which represents a potential threat to the growth of digital marketing and e-commerce. If a company wants to be successful in consumer markets, consumer privacy needs to be addressed in a responsible manner, while ignoring consumer privacy concerns is considered to be a dangerous business strategy (Beveridge, Cook, and Stubbings, 2015). Reducing privacy concern and increasing consumer confidence in using digital technologies and the acceptance of digital marketing initiatives seem to be an essential priority for companies operating online. Understanding consumer privacy concern, its drivers, implications and situations when privacy matters provides a foundation for developing effective policies and practices to reduce this concern (De Pechpeyrou and Nicholson, 2012).

Privacy concern can be reduced by providing the consumers the ability to control information collection and dissemination. Companies should work to improve consumer attitudes towards the websites of companies in terms of the positive perceptions of comfort, satisfaction and likeness of surfing the web, building relationships with companies and quality of services provided online. Improved privacy policy and informativeness of Websites might also decrease online privacy concern. Companies should also provide transparent data privacy policies to build trust and loyalty. Online marketers should assure the public that consumer information will not be tracked and traded without the individual consumer's knowledge or consent (Krohn, Luo, and Hsu, 2002). Companies might alto obtain and display privacy-related certificates and logos conferred by credible third-party organisations, which might provide guarantee that transactions on the web are safe, and as a result online privacy concern might decrease. Privacy policy should be communicated to public in order to increase consumer awareness (Lwin, Wirtz, and Williams, 2007). Furthermore, marketers should routinely

inform consumers when individual-specific information is collected, let them know how the information will be used, and tell them who will have access to the data. Such efforts are of particular importance when they are targeting groups with high online privacy concern, such as women, older consumers, low-income consumers, less-educated consumers, and individuals with negative previous online experience. Finally, some government intervention is also needed to address the protection of customer data from abuse and to ensure that the data is secure, accurate and used only for the purpose for which it was collected.

Future studies might take into consideration various situations and industry sectors in which privacy can pose a threat. Researchers might investigate consumer behaviour consequences of online privacy concern more in detail, including satisfaction, loyalty, purchases of various products, related to different types of sensitive information. More studies need to be done in relatively underdeveloped countries.

10.5. Challenges for digital marketing related to online privacy concern

Extensive literature review on privacy issues in the commercial setting reveals many challenges that marketers are facing nowadays. This is particularly true for digital marketers, who are introducing new, intrusive, IT-based marketing tactics on a daily basis. Therefore, in this section we are presenting a review of several specific challenges for digital marketing that are related to online privacy concerns.

Digital marketing is currently one of the most dynamic fields of marketing theory and practice. It is defined as “achieving marketing objectives through applying digital technologies” (Chaffey and Ellis-Chadwick, 2012:10). The emergence of digital marketing is a result of vast acceptance of digital platforms by consumers; first desktop (computers), then mobile (smartphone, tablet), and nowadays wearable devices (e.g. smart watches). The usage of various digital technologies leads to the digitalization of consumers’ lives, influencing further development of the field of digital marketing. At the same time, the intrusive nature of these technologies (especially mobile digital devices and wearables) raises many privacy-related

concerns among consumers (Sipior, Ward, and Volonino, 2014). Therefore, it is important to identify how the proliferation of mobile digital devices brings new challenges for digital marketers in the context of online privacy concerns.

The field of mobile marketing emerged as a result of an explosion of mobile phones acceptance since the beginning of the 2000s. It is considered as a sub-field of digital marketing and has attracted a considerable attention of digital marketing researchers (Varnali and Toker, 2010). Although there is still no consent on the comprehensive definition of mobile marketing, it encompasses the use of mobile medium as a means of marketing communication (Leppaniemi, Sinisalo, and Karjaluoto, 2006, Shankar and Balasubramanian, 2009), mobile commerce and mobile social network management (Shankar, Venkatesh, Hofacker, and Naik, 2010). Smutkupt, Krairit, and Esichaikul (2010) state that mobile devices should no longer be used as just a channel for marketing communication, but they should be seen as a virtual one-to-one marketing channel where marketers engage customers in personalized relationships. Therefore, same authors stress that “due to the personal nature of a mobile device, communication through this channel has a high tendency to invade customer privacy, which could result in a negative influence on customer perception of the brand being promoted.” (Smutkupt, Krairit, and Esichaikul, 2010:136). Consequently, the issue of trust as a major obstacle in adoption of mobile services and m-loyalty becomes one of the focal point of mobile marketing research, and addressing the security/privacy concerns of mobile users is stressed as one of the best strategic practices among mobile marketers (Varnali and Toker, 2010). There are several properties of mobile devices that have key marketing implications, such as: portability/ubiquity, untethered/wireless feature, personalization, two-way communication, and location-specificity (Shankar and Balasubramanian, 2009; Smutkupt, Krairit, and Esichaikul, 2010). The latter has recently raised the most of the privacy concerns among consumers. One the one side, marketing tactics that are leveraging the positional information of the mobile device are more intrusive and contextual, and if they are conducted correctly, they can provide customers with just-in-time, in-context, personalized marketing offers and services (Persaud and Azhar, 2012). But in practice, the loss of location privacy in the age of mobile devices raises severe concerns. Service providers are able to

"obtain location estimates with address-level precision, creating a serious privacy problem, as the estimates can be highly revealing of user behaviour, preferences, and beliefs." (Wicker, 2012, p. 60). Researchers have already identified privacy concerns related to location data. Unni and Harmon (2007) found that mobile phone users express high privacy concerns when receiving ads that were location-based (location-based advertising, LBA), especially when those ads were push-based. Similar study by Limpf and Voorveld (2015) has confirmed that information privacy concerns have a direct negative effect on LBA acceptance, but only in the case of push-based ads. Besides for LBA, mobile devices are increasingly used for the purposes of sales promotion. Therefore, Im and Ha (2015) examined the determinants of permission-granting intention of consumers in the context of mobile couponing, based on transaction utility theory. It was found that perceived privacy risk is driven by fear of spamming (unsolicited messaging), and it is negatively related to mobile coupon permission-grating intention. Besides for communication, mobile devices are nowadays used for mobile purchasing or m-commerce. This has motivated Zhang, Chen, and Lee (2013) to examine the antecedents of privacy concerns in the m-commerce setting. Their study showed that privacy concerns over m-commerce are influenced by age (younger consumers are less concerned) and slightly influenced by education level (less educated consumers are less concerned). However, income level, previous m-commerce experience and gender are found not to have a significant influence on privacy concerns over m-commerce.

Xu, Luo, Carroll, and Rosson (2011) investigated the extended privacy calculus model in the context of location-aware marketing (LAM) and found that perceived value of information disclosure in location-aware marketing activities is a trade-off between perceived value and perceived risks of location information disclosure. Furthermore, perceived value of information disclosure drives willingness to have personal information used in LAM, which finally positively affects purchase intention. Privacy concerns are recognized as an important topic in the context of location-based services (LBS). LBS are services that are based on the usage of mobile devices' location data, in order to provide value for users (Dhar and Varshney, 2011). If a smartphone user wants to use LBS (e.g. a mobile application for searching a free table in nearby restaurants), they have to disclose their location data, i.e. allow the mobile

application to track their whereabouts. Although permission-based, LBS are considered as highly intrusive. Since privacy concerns that are associated with the use of LBS may discourage consumers from gaining the convenience of personalized services, Xu and Gupta (2009) investigated the adoption of LBS through a privacy lens. They found that that privacy concerns significantly influence continued adoption of LBS, as compared to initial adoption. Zhou (2011) also found that privacy concern also has a significant effect on user adoption of LBS. Among four dimensions of privacy concern, collection and secondary use were found to be the main factors affecting perceived risk, and errors were found to be the main factors affecting trust. Trust was found to affect perceived risk, and both factors determined usage intention. Yun, Han, and Lee (2013) investigated the moderating effect of privacy concerns on the influence of performance expectancy, effort expectancy, and social influence on continuous intention to use LBS, as well as the relationship between continuous intention to use LBS and actual use. According to their results, it seems that privacy concerns are not always the main causes of slow LBS diffusion, because the effects of privacy concerns on LBS revealed different patterns depending on what originally motivated the users to use LBS.

While mobile digital devices are becoming ubiquitous, many researchers are calling for more extensive research of privacy concerns in the context of mobile marketing (e.g. Smutkupt, Krairit, and Esichaikul, 2010; Sipior, Ward, and Volonino, 2014). Many properties of mobile digital devices are preventing the mitigation of privacy concerns among consumers, since their operating systems do provide an adequate level of protection for the user's personal data (Tsavli, Efraimidis, Katos, and Mitrou, 2015). This issue is important for all stakeholders in the business arena: consumers, consumers' protection organizations, companies, and policy makers. Privacy concerns research would benefit all of them, and would help in building sustainable models for digital and mobile marketing in the age of data.

Finally, from the marketing point of view, it is interesting to examine how consumers value their personal privacy in the commercial setting. Acquisti, John, and Loewenstein (2013) performed a field experiment to investigate individual privacy valuations. They have found

that consumers value their privacy differently according to how much money they would receive for disclosing otherwise private information, and how much they would pay to protect otherwise public information. Also, the order in which they considered different offers for their data played a significant role. If charging for privacy becomes a common business practice, this could significantly affect marketing aspects of privacy concerns and give a new perspective on the current scientific evidence on the role of privacy concerns in the commercial setting.

11. FOUR YEARS AFTER

The time has come to close this PRICON book although some papers are still pending for publication; some more ideas to exploit the dataset are emerging. We are preparing the final PRICON conference in May 2018 at the Institute of Economics, Zagreb and we would like to show the book to our colleagues and public. For those who could not attend, here we are, the PRICON team again.

The PRICON team 2018

By Branka Domić.

REFERENCES

1. Aarnio, K., and Lindeman, M. (2015). Religious People and Paranormal Believers. Journal of Individual Differences, 28(1), 1-9.
2. Acquisti, A., Leslie, J.K., and Loewenstein, G. (2013). What Is Privacy Worth? The Journal of Legal Studies, 42(2), 249-274.
3. Akhter, S.H. (2014). Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement. Journal of Consumer Marketing, 31(2), 118-125.
4. Allen, J. (2015). Online Privacy and Hacking. San Diego: Reference Point Press.
5. Allmer, T. (2012). Critical Internet Surveillance studies and Economic Surveillance, in Christian Fuchs, Kees Boersma, Anders Albrechtslund, Marisol Sandoval (Eds). Internet and Surveillance, New York: Routledge, 231-246.
6. Altman, I. (1975). The environment and social behaviour. Monterey: Brooks/Cole.
7. Anić, I.-D. (2015). The development of database marketing: does consumer information privacy matter? Zbornik radova Ekonomskog fakulteta Sveučilišta u Mostaru, 21, 39-56.
8. Anić, I.D., Škare, V., and Kursan Milaković, I. (2016). Determinants and behavioural consequences of online privacy concerns among young consumers in Croatia. Ekonomski pregled, 67(5), 377-398.
9. Awad, N. F., and Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization, MIS Quarterly, 30(1), 13-28.
10. Bagozzi, R. P., and Yi, Y. (1988). On the evaluation of structural equation models. Journal of the Academy of Marketing Science, March, 16(1), 74-94.
11. Bandyopadhyay, S. (2009). Antecedents and Consequences Of Consumers' Online Privacy Concerns. Journal of Business and Economics Research, 7(3), 41-48.
12. Bandyopadhyay, S. (2011). Online privacy concerns of Indian consumers. International Business and Economics Research Journal, 10(2), 93-100.
13. Bansal, G., Zahedi, F. M., and Gefen, D. (2010). The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online. Decision Support Systems, 49(2), 138-150.

14. Bansal, G., Zahedi, F., and Gefen, D. (2008). The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation, in Proceedings of 29th International Conference on Information Systems, Paris, France, December 14-17.
15. Bansal, G., Zahedi, F.M., and Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. Information and Management, 53(1), 1-21.
16. Bélanger, F., and Crossler, R.E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly, 35 (4), 1017-1041.
17. Bélanger, F., Hiller, J., and 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.
18. Bellman, S., Johnson, E. J., Kobrin, S., and Lohse, G. L. (2004). International differences in information privacy concerns: a global survey of consumers. The Information Society, 20(5), 313-324.
19. Benett, C. (2011). In defence of privacy: the concept and the regime. Surveillance and Society, 8(4), 485-496.
20. Berg, B. (1995). Qualitative Research Methods for the Social Sciences (2nd edition). Boston: Allyn and Bacon.
21. Bergeman, C. S., Chlpuer, H. M., Plomin, R., Pedersen, N. L., McClearn, G. E., Nesselroade, J. R., Jr. Costa, P. T., and McCrae, R. R. (1993). Genetic and Environmental Effects on Openness to Experience, Agreeableness, and Conscientiousness: An Adoption/Twin Study. Journal of Personality, 61(2), 159–179.
22. Beveridge, A., Cook, C., and Stubbings, A. (2015). Privacy, The Futures Company, http://thefuturescompany.com/free-thinking/privacy/ (accessed 13 January 2016).
23. Boettke, P. J., and Coyne, C. J. (2009). Context matters: Institutions and entrepreneurship. Now Publishers Inc.
24. Bonneau, J., and Preibusch, S. (2010). The privacy jungle: on the market for data protection in social networks. U T. Moore, D. J. Pym, and C. Ioannidis, Economics of Information Security and Privacy (pp. 121-167). New York: Springer.

25. Brashear, T., Milne, G., and Kashyap, V., (2006). Internet Culture And Information Privacy Concerns In Developing Countries. Salvador, Brasil.
26. Buchanan, T., Paine, C., Joinson, A. N., and 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.
27. Buchi, M., Just, N., and Latzer, M. (2016). Caring is not enough: the importance of Internet skills for online privacy protection. Information, Communication and Society, 05 September, 1-18.
28. Budak, J., Rajh, E., and Žokalj, M. (2016). Personal values of Internet users: a cluster analytic approach, working papers EIZ-WP-1606 Available at http://www.eizg.hr/hr-HR/Radni-materijali-EIZ-a-207.aspx (last accessed 20.3.2017)
29. Budak, J., Rajh, E., and Recher, V. (2016). Citizens' privacy concerns: does national culture matter? In Surveillance, Privacy and Security: Citizens' Perspectives. Michael Freidwald, J. Peter Burgess, Johann Čas, Rocco Belanova, Walter Peissl (ur.), Routledge, 2017. pp. 36-51.
30. Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., and Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. Journal of Social and Personal Relationships, 2(6), 131-158.
31. Caudill, E.M., and Murphy, P.E. (2000). Consumer online privacy: Legal and ethical issues. Journal of Public Policy and Marketing, 19(1), pp. 7-19.
32. Cecere, G., Le Guel, F. and Soulie, N. (2015). Perceived Internet privacy concerns on social networks in Europe. Technological Forecasting and Social Change, 96 (July), 277-287.
33. Chaffey, D., and Ellis-Chadwick, F. (2012). Digital Marketing: Strategy, Implementation and Practice, 5th Edition, Harlow: Pearson.
34. Chen, J., Zhang, Y., and Heath, R. (2001). An exploratory investigation of the relationships between consumer characteristics and information pirvacy. Marketing Management Journal, 11(1), 73-81.
35. Chen, K., and Rea, A. (2004). Protecting personal information online: a survey of user privacy concerns and control techniques. Journal of Computer Information Systems,

44(4), 85-92.

36. Chen, L., Liu, H.-W. (2015). A review of privacy protection in e-commerce. Journal of Advanced Management Science, 3(1), 50-53.
37. Chiou, A., Chen, J.-c. V., and Bisset, C. (2009). Cross cultural perceptions on privacy in the United States, Vietnam, Indonesia, and Taiwan. U C. Kuanchin, and A. Fadlalla, Online Consumer Protection: Theories of Human Relativism (284-298). New York: IGI Global.
38. Cho, C.-H., and Cheon, H.J. (2004). Why Do People Avoid Advertising on the Internet?, Journal of Advertising, 33(4), 89–97.
39. Cho, H., Rivera, M. and Lim, S. (2009). A Multinational Study on Online Privacy: Global Concern and Local Responses. New Media and Society, 11(3), 395-416.
40. Clarke, R. (1997). Introduction to Dataveillance and Information Privacy, and Definitions of Terms, Roger Clarke's Web-Site, http://www.rogerclarke.com/DV/Intro.html (accessed 8 January, 2016).
41. Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. Communications of the ACM, 42 (2), 60-67.
42. Clarke, R. (2009). Privacy impact assessment: its origins and development. Computer Law and Security Review, 25(2), 123-135.
43. Cohen, J. (1988). Statistical power analysis for the behavioral sciences. New Jersey: Lawrence Erlbaum.
44. Cullen, R. (2009). Culture, identity and information privacy in the age of digital government. Online Information Review, 33(3), 405-421.
45. De Pechpeyrou, P. and Nicholson, P. (2012). An Integrated Framework for Privacy Concerns in France. International Journal of Integrated Marketing Communications, 4(1), 19-32.
46. DeCew, J. W. (1997). In pursuit of privacy: law, ethics, and the rise of technology. New York: Cornell University Press.
47. Denzin, N. (1978). Sociological Methods: A Source Book (2nd edition). McGraw-Hill.
48. DESI 2015 Country Profile – Croatia, https://ec.europa.eu/digital-single-market/en/scoreboard/croatia Accessed 21.07.2016

49. DESI 2017 Country Profile – Croatia, https://ec.europa.eu/digital-single-market/en/scoreboard/croatia Accessed 21.05.2017
50. Dhar, S., and Varshney, U. (2011). Challenges and Business Models for Mobile Location-based Services and Advertising. Communications of the ACM, 54(5), 121-129.
51. Dinev, T., and Hart, P. (2004). Internet Privacy Concerns and Their Antecedents, Measurement Validity and a Regression Model. Behaviour and Information Technology, 23(6), 413–422.
52. Dinev, T., and Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce, 10(2), 7-29.
53. Dinev, T., and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions, Information Systems Research, 17(1), 61–80.
54. Dinev, T., Bellotto, M., Hart, P., Russo. V., Serra, I., and Colautt, C. (2006). Privacy Calculus Model in E-Commerce - A Study of Italy and the United States. European Journal of Information Systems, 15(4), 389 - 402.
55. Dinev, T., Masssimo, B., Hart, P., Christian, C., Vincenzo, R., and 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. Proceedings of the 18th Bled eConference: eIntegration in Action, 30. Bled, Slovenia.
56. Dolnicar, S., and Jordaan, Y. (2007). A Market-Oriented Approach to Responsibly Managing Information Privacy Concerns in Direct Marketing. Journal of Advertising, 36(2), 123-149.
57. Dommeyer, C., and 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), pp. 34-51.
58. Donnellan, M. B., Oswald, F. L., Baird, B. M., and Lucas, R. E. (2006). The Mini-IPIP Scales: Tiny-yet-effective measures of the Big Five Factors of Personality. Psychological Assessment, 18(2), 192-203.
59. Dorfman, P., and Howell, J. (1988). Dimensions of national culture and effective leadership patterns: Hofstede revisited. Advances in Comparative International Management, 3,

127-149.

60. Eastlick, M.A., Lotz, S. L., and Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. Journal of Business Research, 59(8), 877-886.
61. eMarketer (2016). Worldwide Retail Ecommerce Sales: The eMarketer Forecast for 2016. Available at: https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369#sthash.43pnUme0.dpuf (last accessed 20.3.2017)
62. Ess, C., and Sudweeks, F. (2005). Culture and Computer-Mediated Communication: Toward New Understandings. Journal of Computer-Mediated Communication, November, 11(1), 179-191.
63. Etzioni, A. (1999). The limits of privacy. New York: Basic Books.
64. European Commission (2011). Attitudes on Data Protection and Electronic Identity in the European Union, Special Eurobarometer, 359 http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (accessed 13 January 2016).
65. European Commission (2013). Europe 2020: Europe's growth strategy, Luxembourg: Publications Office of the European Union.
66. European Commission (2016). Eurostat.
67. Faja, S., and Trimi, S. (2006). Influence of the Web Vendor's Interventions on Privacy-Related Behaviours in E-Commerce. Communications of the Association for Information Systems, 17 (Article 27), 593–634.
68. Featherman, M. S., and Pavlou, P. A. (2003). Predicting E-Services Adoption: A Perceived Risk Facets Perspective. International Journal of Human-Computer Studies, 59(4), 451-474.
69. Flaherty, D. H. (1989). Protecting privacy in surveillance societies: the federal Republic of Germany, Sweden, France, Canada, and the United States. UNC Press Books.
70. Fogel, J., and Nehmad, E. (2009). Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns. Computers in Human Behaviour, 25(1), 153–160.
71. Fornell, C., and Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39-50.

72. Fornell, C., and F. L. Bookstein (1982). Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory. Journal of Marketing Research, 19(4), 440-452.
73. Fuchs, C. (2012). The political economy of privacy on facebook. Television and New Media, 13(2), 139-159.
74. Gaunt, R. (2006). Couple Similarity and Marital Satisfaction: Are Similar Spouses Happier?. Journal of Personality, 74(5), pp. 1401-1420.
75. Gellman, R., and Dixon, P. (2011). Online privacy: a reference handbook. Santa Barbara: ABC Clio.
76. Gerbing, D. W., and Anderson, J. C. (1988). An Updated Paradigm for Scale Development Incorporating Unidimensionality and Its Assessment. Journal of Marketing Research, 25(2), 186-192.
77. Goldberg, L. R. (1992). The development of markers for the Big-Five factor structure. Psychological Assesment, 7(1), 26-42.
78. Goodwin, C. (1991). Privacy: Recognition of a consumer right. Journal of Public Policy and Marketing, 10(1), 149-166.
79. Goold, B. (2009). Surveillance and the political value of privacy. Amsterdam Law Forum, 4(1), 3-6.
80. Goold, B. (2010). How much surveillance is too much? Some thoughts on surveillance, democracy and the political value of privacy. U D. Schartum, Surveillance in a Constitutional Government (38-48). Fakbokforlaget.
81. Graeff, T.R., and Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. Journal of Consumer Marketing, 19(4), 302 – 318.
82. Grubbs Hoy, M., and Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. Journal of Interactive Advertising, 10(2), 28-45.
83. Gurung, A., and Jain, A. (2009). Antecedents of online privacy protection behaviour: towards an integrative model. U K. Chen, and A. Fadlalla, Online Consumer Protection: Theories of Human Relativism (151-190). New York: IGI Global.
84. Haggerty, K., and Gazso, A. (2005). The public politics of opinion research on surveillance and privacy. Surveillance and Society, 3(2/3), 173-180.
85. Haggerty, K.D. , and Ericson, R.V. eds., (2006). The New Politics of Surveillance and

Visibility. Toronto: University of Toronto Press.

86. Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. (2014). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Thousand Oaks: Sage.
87. Hartmann, M. (2011). Mobile privacy: contexts. U S. Trepte, and L. Reinecke, Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web (str. 191-203). Berlin: Springer.
88. Heirman, W., M. Walrave, K. Ponnet, and Van Gool, E. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicatbility of a trust-based model, Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7(3), 1-23.
89. Henderson, H. (2015). Online Privacy and Government. San Diego: Reference Point Press.
90. Henseler, J., and Sarstedt, M. (2013). Goodness-of-fit indices for partial least squares path modeling. Computational Statistics, 28(2), 565–580.
91. Hin, S. S., Tanamal, T. K. Y. M., Yi, H. J., Ling, L. W., Yahya, M. M., and Ho, J. S. Y. (2015). Consumer Personality, Privacy Concerns and Usage of Location-Based Services (LBS). Journal of Economics, Business and Management, 3(10), 961-966.
92. Hoffman, D., Novak, T., and Peralta, M. (1999). Information privacy in the marketspace: Implications for the commercial uses of anonymity on the web. The Information Society, 15(4), 129-139.
93. Hofstede, G. (1980). Culture's Consequences: International Differences in Work Related Values. Beverly Hills, CA: Sage Publications.
94. Hofstede, G., Hofstede, G. J., and Minkov, M. (2010). Cultures and organizations: Software of the mind (3rd ed.), New York: McGraw Hill.
95. Hoy, G.M., and Milne, G. (2010). Gender differences in privacy-related measures for young adult facebook users. Journal of Interactive Advertising, 10(2), 28-45.
96. Hsu, C.-w. J. (2009). Privacy or performance matters on the internet: revisiting privacy toward a situational paradigm. U K. Chen, and A. Fadlalla, Online Consumer Protection: Theories of Human Relativism (str. 214-238). New York: IGI Global.
97. Hu, L.-t., and Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure

analysis: Conventional criteria versus new alternatives. Structural Equation Modeling: A Multidisciplinary Journal, 6(1), 1-55.

98. Hui, K.L., and Png, I.P.L. (2006). The Economics of Privacy, In Hendershott, E. (Ed.), Handbooks in Information Systems (1-27). Amsterdam: Elsevier B.V.
99. Ifinedo, P., 2011. Relationships between information security concerns and national cultural dimensions: findings in the global financial services industry. In H. R. Nemati, Security and Privacy Assurance in Advancing Technologies (pp. 134-153). Hershey-New York: Information Science Reference.
100. Inness, J. C. (1996). Privacy, intimacy, and isolation. New York: Oxford University Press.
101. Janda, S., and Fair, L. (2004). Exploring consumer concerns related to the Internet. Journal of Internet Commerce, 3(1), 1-21.
102. Ji, P., and Lieber, P. (2010). Am I safe? Exploring relationships between primary territories and online privacy. Journal of Internet Commerce, 9(1), 3-22.
103. Joinson, A., Reips, U., Buchanan, T., and Schofield, C. B. (2010). Privacy, trust and self-disclousre online. Human-Computer Interaction, 25(1), 1-24.
104. Judge, T. A., Heller, D., Mount, M. K., 2002. Five-Factor Model of Personality and Job Satisfaction: A Meta-Analysis. Journal of Applied Psychology, 87(3), 530-541.
105. Junglas, I., Johnson, N., and Spitzmuller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based service. European Journal of Information Systems, 17(4), 387-402.
106. Kiryanova, B.E., and Makienko, I. (2011). The effects of information privacy and online shopping experience in e-commerce. Academy of Marketing Studies Journal, 15(1), 97-112.
107. Korgaonkar, P.K., and Wolin, L.D. (1999). A multivariate analysis of web usage. Journal of Advertising Research, 39(2), 53-68.
108. Korzaan, M. L., and Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioural intentions. Journal of Computer Information Systems, 48(4), 15-24.
109. Kosinski, Michal; Stillwell, D., and Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behaviour, Proceedings of the National

Academy of Sciences, 110 (15), 5802–5805.

110. Krohn, F., Luo, X., and Hsu, M.K. (2002). Information Privacy and Online behaviour. Journal of Internet Commerce, 1(4), 55-69.

111. Kumar, V., and Reinartz, W. (2012). Consumer relationship management, New York: Springer.

112. Kumaraguru, P., and Cranor, L. (2006). Privacy in India: attitudes and awareness. U I. Goldberg, and M. Atallah, Privacy Enhancing Technologies (str. 243-258). Berlin: Springer Berlin Heidelberg.

113. Leppäniemi, M., Sinisalo, J., and Karjaluoto, H. (2006). A Review of Mobile Marketing Research. International Journal of Mobile Marketing, 1(1), 30-40.

114. Lewis, K. (2011). The co-evolution of social network ties and online privacy behaviour. U S. Trepte, and L. Reinceke, Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web (91-109). Berlin: Springer.

115. Li, S., and Zhang, C. (2009). An empirical investigation of information privacy concern and its antecedents and consequences, Proceedings for the Northeast Region Decision Sciences Institute (NEDSI), 344-349.

116. Li, Y. (2011). Empirical studies on online information privacy concerns: literature review and an integrative framework. Communications of the Association for Information Systems, 28(1), 453-496.

117. Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity. Journal Decision Support System, 57(1), 343-354.

118. Li, Y. (2011). Empirical studies on online information privacy concerns: literature review and an integrative framework. Communications of the Association for Information Systems, 28(1), 453-496.

119. Lili, W., and Min, D. (2014). Effect of Cultural Factors on Online Privacy Concern. Journal of Information Technology Applications and Management, 21(2), 149-165.

120. Lilien, L., and Bhargava, B. (2009). Privacy and trust in online interactions. U K. Chen, and A. Fadlalla, Online Consumer Protection: Theories of Human Relativism (85-122). Hershey: IGI Global.

121. Limpf, N., and Voorveld, H.A.M. (2015). Mobile Location-Based Advertising: How

Information Privacy Concerns Influence Consumers' Attitude and Acceptance. Journal of Interactive Advertising, 15(2), 111-123.

122. Lindeman, M., Verkasalo, M., (2005). Measuring Values With the Short Schwartz's Value Survey, Journal of Personality Assessment, 85(2), 170-178.
123. Liu, C., Marchewka, J., Lu, J., and Yu, C. (2004). Beyond concern: a privacy-trust-behavioural intention model of electronic commerce. Information and Management, 42(1), 127-142.
124. Lwin, M., J., Wirtz, and 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.
125. Lyon, D. (1994). The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press.
126. Malhotra, N., Kim, S., and Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale and a causal model. Information System Research, 15(4), 336-355.
127. Markos, E., Labrecque, L.I and Milne, G.R. (2012). Web 2.0 and consumers' digital footprint: managing privacy and disclosure choices in social media. In Close A.G. (Ed.), Online consumer behaviour: theory and research in social media, advertising, and e-tail (pp. 157-182). New York: Routledge.
128. Mathiyalakan, S., Taylor, G., Heilman, G.E., White, S., Brusa, J., and Guitierrez, P.C. (2014). Online Privacy Concerns: Gender Differences among Hispanic Undergraduate Students, Review of Business Research, 14(2), 83-88.
129. McCrae, R. R., and Costa, P. T., 1987. Validation of the Five-Factor Model of Personality Across Instruments and Observers. Journal of Personality and Social Psychology, 52(1), pp. 81-90.
130. McCrae, R. R., and Costa, P. T., 1991. Adding liebe and arbeit: the full five-factor model and well-being. Personality and Social Psychology Bulletin, 17(2), pp. 227-232.
131. Mediati, N. (2010). The Most Dangerous Places on the Web, PC World, 28(11), 72–80.
132. Metzger, M., and Docter, S. (2003). Public opinion and policy initiatives for online privacy protection, Journal of Broadcasting and Electronic Media, 47(3), 350–374.

133. Metzger, M. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce, Journal of Computer-Mediated Communication, 9(4).

134. Milberg, S. J., Smith, J. H., and Burke, S. J. (2000). Information privacy: corporate management and national regulation. Organization Science, 11(1), 35-57.

135. Miles, M., and Huberman, A. (1994). An Expanded Sourcebook: Qualitative Data Analysis (2nd edition). Sage Publications.

136. Milne, G. R., Rohm, A. J., and Bahl, S. (2004). Consumers' protection of online privacy and identity. Journal of Consumer Affairs, 38(2), 217–232.

137. Milne, G.R., and Boza, M.E. (1999). Trust and Concern in consumers' perceptions of marketing information management practices. Journal of Interactive Marketing, 13(1), 5-24.

138. Milne, G.R., Beckman, J., and Taubman, M.L. (1996). Consumer Attitudes toward Privacy and Direct Marketing in Argentina. Journal of Direct Marketing, 10(1), 22-33.

139. Milne, G.R., Gabisch, J.A., Markos, E., and Phelps, J.E. (2012). Changes in Consumer Willingness to Provide Information over the Last Decade: A Cohort Analysis. International Journal of Integrated Marketing Communications, 4(2), 44-59.

140. Miltgen, C. and Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy. European Journal of Information Systems, 23(2), 103-125.

141. Miyazaki, A. D., and Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. Journal of Consumer Affairs, 36(1), 28–49.

142. Miyazaki, A., and Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. The Journal of Consumer Affairs, 35(1), 27-44.

143. Moore, B. (1984). Privacy: studies in social and cultural history. New York: M.E. Sharpe.

144. Morimoto, M., and Macias, W. (2009). A Conceptual Framework for Unsolicited Commercial E-mail: Perceived Intrusiveness and Privacy Concerns. Journal of Internet Commerce, 8(3/4), 137-160.

145. Morton, A., 2013. Measuring Inherent Privacy Concern and Desire for Privacy - A Pilot Survey Study of an Instrument to Measure Dispositional Privacy Concern. Washington DC, Usa, IEEE Computer Society Washington.

146. Naef, M., and Schupp, J. (2009). Measuring Trust: Experiments and Surveys in Contrast and Combination, IZA Discussion Paper Series, IZA DP No. 4087, Bonn: Institute for the Study of Labor (IZA).
147. Nam, C., C. Song, E. Lee, and C.I. Park (2006). Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online. Advances in Consumer Research, 33(1), 212-217.
148. Nemati, H. R. (2011). Preface. In H. R. Nemati, Security and Privacy Assurance in Advancing Technologies. Hershey-New York: Information Science Reference.
149. North, D. (2000). Big-Bang Transformations of Economic Systems: An Introductory Note. Journal of Institutional and Theoretical Economics, 156(1), 3-8.
150. O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. Social Science Computer Review, 19(1), 17-31.
151. Okazaki, S., Li, H., and Hirose, M. (2009). Consumer Privacy Concerns and Preference for Degree of Regulatory Control. Journal of Advertising, 38(4), 63-77.
152. Osatuyi, B. (2015). Personality Traits and Information Privacy Concern on Social Media Platforms. Journal of Computer Information Systems, 55(4), 11-19.
153. Parasuraman, S. and 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.
154. Patton, J. (2000). Protecting privacy in public? Surveillance technologies and the value of public places. Ethics and Information Technology, 2(3), 181-187.
155. Pauxtis, A., and White, B. (2009). Google: technological convenience vs. technological intrusion. U K. Chen, and A. Fadlalla, Online Consumer Protection: Theories of Human Relativism (1-16). London: IGI Global.
156. Pavlou, P. A. (2011). State of the information privacy literature: where are we now and where should we go? MIS Quearterly, 35(4), 977-988.
157. Pavlou, P. A. (2002). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. International Journal of Electronic Commerce, 7(3), 101-134.
158. Pavlou, P.A., Fygenson, M. (2006). Understanding and predicting electronic commerce

adoption: An extension of the theory of planned behaviour. MIS Quarterly, 30(1), 115-143.

159. Pavlou, P.A., Liang, H., and Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: a principal- agent perspective, MIS Quarterly, 31(1), 105-136.

160. PCWorld (2013). The 5 biggest online privacy threats of 2013", http://www.pcworld.com/article/2031908/the-5-biggest-online-privacy-threats-of-2013.html (accessed 8 January 2016).

161. Persaud, A., and Azhar, I. (2012). Innovative mobile marketing via smartphones. Are consumers ready? Marketing Intelligence and Planning, 34(4), 418-443.

162. Phelps, J.E., D'Souza, G., and Nowak, G.J. (2001). Antecedents and Consequences of Consumer Privacy Concerns: an Empirical Investigation. Journal of Interactive Marketing, (15), 4, 2-17.

163. Pingitore, G., Meyers, J., Clancy, M., and Cavallaro, K. (2013). Consumer Concerns About Data Privacy Rising: What Can Business Do?, McGraw Hill Financial/Global Institute, http://www.jdpower.com/sites/default/files/Consumer_Concerns_Data_Privacy.pdf (accessed December 5, 2017, pp. 1-17).

164. Poortinga, W., Spence, A., Whitmarsh, L., Capstick, S., and Pidgeon, N. F. (2011). Uncertain climate: An investigation into public scepticism about anthropogenic climate change. Global Environmental Change, 21(3), 1015-1024.

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

166. Rammstedt, B., and John, O. P., 2007. Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German. Journal of Research in Personality, 41(1), 203-212.

167. Ranzini, G., Etter, M., Lutz, C., and Vermeulen, I.E. (2017). Privacy in the Sharing Economy, Report from the EU H2020 Research Project Ps2Share: Participation, Privacy, and Power in the Sharing Economy, http://dx.doi.org/10.2139/ssrn.2960942 (accessed December 5, 2017), 1-19.

168. Rea, A., and Chen, K. (2009). Privacy control and assurance: does gender influence online information exchange. U K. Chen, and A. Fadlalla, Online Consumer Protection:

Theories of Human Relativism (165-189). New York: IGI Global.

169. Reay, I., Beatty, P., Dick, S., and Miller, J. (2013). Privacy policies and national culture on the internet. Information Systems Frontiers, 15(2), 279-292.
170. Recher, V., Budak, J., and Rajh, E. (2016). Development in digital and post-transition era: online privacy concern approach, 4th REDETE Conference Economic Development and Entrepreneurship in Transition Economies : Assessment of the last 25 years, going beyond the 'transition': proceedings. Banja Luka: Faculty of Economics, University of Banja Luka, 2016. 1225-1237.
171. Reed, T. (2014). Digitized Lives: Culture, Power and Social Change in the Internet Era. New York and London: Taylor and Francis; Routledge.
172. Regan, P. (1995). Legislating privacy: technology, social values and public policy. Chapel Hill: Blackwell Publishing.
173. Regan, P. M. (2002). Privacy as a Common Good in the Digital World. Information, Communication and Society, 5(3), 382-405.
174. Rice, R.E. (2006). Influences, usage, and outcomes of Internet health information searching: Multivariate results from the Pew surveys. International Journal of Medical Informatics, 75(1), 8–28.
175. Ringle, C. M., Wende, S., and Will A. (2005). SmartPLS 2.0.M3. Hamburg: SmartPLS, http://www.smartpls.de (accessed February 22, 2017)
176. Rust, R., Kannan, P. K., and Peng, N. (2002). The customer economics of internet privacy. Journal of Academy of Marketing Science, 30(4), 455–464.
177. Saher, M., and Lindeman, M. (2005). Alternative medicine: A psychological perspective. Personality and Individual Differences, 39(6), 1169-1178.
178. Salgado, J. F., Moscoso, S., and Lado, M.(2003). Evidence of cross-cultural invariance of the big five personality dimensions in work settings. European Journal of Personality. 17(1), 67-76.
179. Sanchez, G. (2013). PLS Path Modeling with R. Berkeley: http://www.gastonsanchez.com/PLS Path Modeling with R.pdf.
180. Sanchez, G., Trinchera, L., and Russolillo, G. (2015). plspm: Tools for Partial Least Squares Path Modeling. R package version 0.4.7.,

https://CRAN.R-project.org/package=plspm.

181. SAS, Big Data – What Is It?, http://www.sas.com/en_us/insights/big-data/what-is-big-data.html (accessed 8 January, 2016).
182. Schoenbachler, D.D., and Gordon, G.L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. Journal of Interactive Marketing, 16(3), 2-16.
183. Schwartz, S. H. (2012). An Overview of the Schwartz Theory of Basic Values. Online Readings in Psychology and Culture, 2(1) 1-20.
184. Schwartz, S. (1992). Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries. Advances in Experimental Social Psychology, 25(1), 1-65.
185. Shaiq, H., Khalid, H., Akram, A., and Ali, B. (2011). Why not everybody loves Hofstede? What are the alternative approaches to study of culture? European Journal of Business and Management , 3(6), 101-111.
186. Shankar, V., and Balasubramanian, S. (2009). Mobile Marketing: A Synthesis and Prognosis, Journal of Interactive Marketing, 23, 118-129.
187. Shankar, V., Venkatesh, A., Hofacker, C., and Naik, P. (2010). Mobile Marketing in the Retailing Environment: Current Insights and future Research Avenues. Journal of Interactive Marketing, 24, 111-120.
188. Sheehan, B.K. (1999). An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviour. Journal of Interactive Marketing, 13(4), 24-38.
189. Sheng, H., F.F. Nah, and Siau, K. (2008). An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personal Personalization and Privacy Concerns. Journal of the Association for Information Systems, 9(6), 344–376.
190. Silverman, D. (2006). Interpreting Qualitative Data (3rd edition). Sage Publications.
191. Sipior, J.C., Ward, B.T., and Volonino, L. (2014). Privacy Concerns Associated with Smartphone Use, Journal of Internet Commerce, 13(3-4), 177-193.
192. Smith, H.J., Milberg, S.J., and Burke, S.J. (1996). In-formation Privacy: Measuring, Individuals' Concerns about Organisational Practices. MIS Quarterly, 20(2), 167–196.
193. Smith, J. H., Dinev, T., Xu, H. (2011). Information privacy research: An interdisciplinary

review. MIS Quarterly, 35(4), 989-1015.

194. Smutkupt, P., Krairit, D., and Esichaikul, V. (2010). Mobile Marketing: Implications for Marketing Strategies. International Journal of Mobile Marketing, 5(2), 126-139.

195. Solove, D. (2008a). Understanding privacy. Harvard: Harvard University Press.

196. Solove, D. J. (2006). Taxonomy of privacy. University of Pennsylvania law review, 154(3), 477-564.

197. Solove, D. J. (2008b). The new vulnerability: data security and personal information. U A. Chander, L. Gelman, and M. J. Radin, Securing Privacy in the Internet Age (111-137). Stanford: Stanford University Press.

198. Son, J., and Kim, S.S. (2008). Internet Users' Information Privacy-Protective Responses: Taxonomy and a Nomological Model. MIS Quarterly, 32(3), 503–529.

199. Stalder, F. (2002). Opinion: Privacy is not the antidote to surveillance. Surveillance and Society, 1(1), 120-124.

200. Stewart, K. A., and Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. Information Systems Research, 13(1), 36-49.

201. Sumner, C., Byers, A., and Shearing, M. (2011). Determining personality traits and privacy concerns from Facebook activity. Black Hat Briefings, Abu Dhabi, United Arab Emirates. Available at: https://media.blackhat.com/bh-ad-11/Sumner/bh-ad-11-Sumner-Concerns_w_Facebook_WP.pdf (last accessed 20.3.2017)

202. Tavani, H. (2008). Informational privacy: concepts, theories, and controversies. U H. T. Tavani, and K. Himma, The Handbook of Information and Computer Ethics (131-164). New Jersey: John Wiley and Sons.

203. Tavani, H. T. (2010). Ethics and technology: controversies, questions, and strategies for ethical computing. New Jersey: John Wiley and Sons.

204. Tenenhaus, M., Vinzia, V. E., Chatelin, Y.-M., and Laurob, C. (2005). PLS path modeling. Computational Statistics and Data Analysis, 48, 159-205.

205. The Futures Company (2012). Privacy: From data to people, http://www.kantarfutures.com/privacy/ (accessed December 5, 2017), 1-28.

206. The Lares Institute, 2011, The Demographics of Privacy — A Blueprint for Understanding Consumer Perceptions and Behavior,

http://www.laresinstitute.com/wp-content/uploads/2011/09/Demographics-Study.pdf (accessed February 22, 2017).

207. Thomas, J. (1994). Factors affecting computer anxiety and its effects on ease of use of business software. Managing Social and Economic Change with Information Technology, Proceedings of 1994 Information Resources Management Association. International Conference, Mehdi Khosrowpour (Ed.), 51-52. London, U.K.: IDEA Group Publishing.
208. Thomas, R.E., and Maurer, V.G. (1997). Database Marketing Practice: Protecting Consumer Privacy. Journal of Public Policy and Marketing, 16(1), 147-155.
209. Tsavli, M., Efraimidis, P.S., Katos, V., and Mitrou, L. (2015). Reengineering the user: privacy concerns about personal data on smartphones, Information and Computer Security, 23(4), 394-405.
210. Tupes, E.C., and Christal, R.E. (1961). Recurrent personality factors based on trait ratings. USAF ASD Tech. Rep. No. 61-97, Lackland Airforce Base, TX: U. S. Air Force. Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/267778.pdf (last accessed 20.3.2017)
211. Ur, B., and 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 (755-762). International World Wide Web Conferences Steering Committee.
212. Vagias, W.M. (2006). Likert-type scale response anchors. Clemson International Institute for Tourism and Research Development, Department of Parks, Recreation and Tourism Management. Clemson University.
213. Varnali, K., and Toker, A. (2010). Mobile marketing research: The-state-of-the-art, International Journal of Information Management, 30, 144-151.
214. Viseu, A., Clement, A., and Aspinall, J. (2004). Situating Privacy Online. Information, Communication and Society, 7(1), pp.92-114.
215. Wall, D. (2006). Surveillant Internet technologies and the Growth in Information Capitalism: Spams and Public Trust in the Information Society, In The new politics of surveillance and visibility, Kevin D. Haggerty, Richard V. Ericson (Eds.), Toronto: University of Toronto Press Inc., 340-362.
216. Walther, J. B. (2011). Introduction to privacy online. U S. Trepte, and L. Reinecke, Privacy Online: Perspectives on privacy and Self-Disclosure in the Social Web (3-7).

Berlin: Springer.

217. Wang Y.D., and Emurian,H.H. (2005). An overview of online trust: Concepts, elements, and implications. Computers in Human Behaviour , 21(1), 105–125.

218. Wang, H., Lee, M.K.O, and Wang, C. (1998). Consumer privacy concerns about Internet marketing. Communications of the ACM, 41(3), 63–70.

219. Wang, P., and Petrison, L.A. (1993). Direct marketing activities and personal privacy. A consumer survey. Journal of Direct Marketing, 7(1), 7–19.

220. Wang, Q., Dacko, S., and Gad, M. (2008). Factors Influencing Consumers' Evaluation and Adoption Intention of Really-New Products or Services: Prior Knowledge, Innovativeness and Timing of Product Evaluation, NA - Advances in Consumer Research Volume 35, eds. Angela Y. Lee and Dilip Soman, Duluth, MN : Association for Consumer Research, pp: 416-422. http://www.acrwebsite.org/volumes/13522/volumes/v35/NA-35

221. Warren, S. D., and Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220.

222. Webster, William, Doina Balahur, Nils Zurawski, Kees Boersma, Bence Sagvari, Christel Backman, (Eds.) 2011, Living in Surveillance Societies: The Ghosts of Surveillance, Proceedings of LiSS Conference 2, Iasi: Editura Universitatii A"l. I. Cuza".

223. Westin, A. F. (1970). Privacy and Freedom. 1st edition, 1967. New York: Atheneum.

224. Westin, A. F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2), 431–453.

225. Whitson, J. (2010). Surveillance and democracy in the digital enclosure, in Kevin D. Haggerty and Minas Samatas, (Eds.) Surveillance and Democracy, Milton Park: Routledge, 231-246.

226. Wicker, S.B. (2012). The Loss of Location Privacy in the Cellular Age. Communications of the ACM, 55(8), 60-68.

227. Wikipedia, Internet privacy, https://en.wikipedia.org/wiki/Internet_privacy (accessed 8 January, 2016).

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

229. Wright, D., and de Hert, P. Eds., (2012). Privacy impact assessment. New York: Springer.
230. Xu, H., and Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services, Electron Markets, 19, 137–149.
231. Xu, H., Dinev, T., Smith, J. H., and Hart, P. (2008). Examining the formation of individual's privacy concerns: toward an integrative view. Proceedings of the 29th International Conference on Information Systems. Paris, France: AISC.
232. Xu, H., Luo X. (R.), Carroll, J. M., and Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems, 51, 42-52.
233. Yao, M. Z. (2011). Self-protection of online privacy: a behavioural approach. U S. Trepte, and L. Reinecke, Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web (111-125). Berlin: Springer.
234. Yao, M.Z., Rice, R.E., and Wallis, K. (2007). Predicting User Concerns about Online Privacy, Journal of the American Society for Information Science and Technology, 58(5), 710-722.
235. Yun, H., Han, D., and Lee, C.C. (2013). Understanding the use of location-based service applications: Do privacy concerns matter? Journal of Electronic Commerce Research, 14(3), 215-230.
236. Zhang, R., Chen, J.Q., and Lee, C.J. (2013). Mobile commerce and consumer privacy concerns. Journal of Computer Information Systems, 53(4), 31-38.
237. Zhang, Y., Chen, J., and 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.
238. Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services, Industrial Management and Data Systems, 111(2), 212-226.
239. Ziesak, J. (2012). The dark side of personalization: online privacy concerns influence customer behaviour. Hamburg: Anchor Academic Publishing.
240. Zmerli, S., and Hooghe, M. (Eds) (2013), Political trust: Why context matters. ECPR Press

241. Zukowski, T., and I. Brown (2007). Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns (paper presented at the conference), in: SAICSIT '07, Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, 197-204. ACM New York, NY, USA.
242. Zureik, E. (2004). Globalization of personal data project international survey concept paper. The Surveillance Project Public Opinion Workshop, 3 March 2004, Kingston, ON.
243. Zviran, M. (2008). User's Perspectives on Privacy in Web-Based Applications. Journal of Computer Information Systems, 48(4), 97–105.

LIST OF FIGURES

LIST OF TABLES

APPENDIX

A. Semi – structured interviews guide

Semi – structured interview guide – PRICON

General about Internet usage

- For what purposes do you use Internet?
- How much time do you usually spend on the Internet?
- When did you start using Internet?
- What devices do you use to connect to the Internet?

Privacy concerns

- Is there any aspect of using internet or is related with using Internet that concerns you?
- (If respondent doesn't specify privacy, ask): Are you concerned about your privacy on the Internet? Why?
- (If respondent specifies privacy concerns, ask): Are you trying to protect you privacy on Internet? In what way? Is that making you less concerned?

Behaviour change

- Did you change your behaviour on the Internet due to privacy concerns? In what way?
- When you wouldn't be concerned about your privacy on Internet, would you behave differently? In what way?
- Are there any activities that you don't want to perform on the Internet due to privacy concerns? Which activities?

Reducing privacy concerns

- In your opinion, are there any ways to reduce your privacy concerns? In what ways?

Interview date: _____ Interview duration:_____

Examinee: code _____ (write in initials and ordinal number of examinee, e.g (JB1))

Sex M F Age _____ Place of residence _____

Education level a) primary school or less b) secondary school c) faculty

Profession _____ (retired, student, unemployed or job position)

B. Questionnaire in English

Dear Sir / Madam, The Institute of Economics, Zagreb conducts a survey-based research on the public opinion about the Internet. Your participation to our research is highly appreciated. Please note that the survey is anonymous and your answers will be presented in the aggregate form only (e.g. in tables with percentages).

1. Are you an Internet user? (on any device e.g. smartphone, computer, etc.)
   - Yes
   - No

If YES, continue If NO, stop the interview (F)

2. (T) Please estimate how many hours in a typical day you spend on the Internet? _____ hours

3. (WEB) For which of the following do you use the Internet?

Receiving and sending e-mails	Yes	No
Using chat/instant message services (e.g. WhatsApp)	Yes	No
Downloading music and/or movies from the internet	Yes	No
Playing online games	Yes	No
Paying bills / e-banking	Yes	No
Attending online courses	Yes	No
Online shopping / internet purchase	Yes	No
Listening to the radio over the internet (streaming)	Yes	No
Watching video over the internet (e.g. YouTube)	Yes	No
Making phone calls over the internet (e.g. Skype, Viber)	Yes	No
Using social networks (e.g. Facebook, Twitter, Instagram)	Yes	No
Following daily news online	Yes	No
Looking for general information on the internet (e.g. Google, Wikipedia)	Yes	No
Using online forums	Yes	No
Using public services available online (e.g. tender applications, fill-in the online forms, filing taxes online, etc.)	Yes	No

4. (FUT) In the future, to what extent do you plan to use Internet: less than today, about the same, more than today?

1 less	2 about the same	3 more

5. (PT) How well do the following statements describe your personality?

1 = Strongly disagree, 2 = Disagree, 3 = Neither agree or disagree,4 = Agree, 5 = Strongly agree					
I see myself as someone who is reserved	1	2	3	4	5
I see myself as someone who is generally trusting	1	2	3	4	5
I see myself as someone who tends to be lazy	1	2	3	4	5
I see myself as someone who is relaxed, handles stress well	1	2	3	4	5
I see myself as someone who has few artistic interests	1	2	3	4	5
I see myself as someone who is outgoing, sociable	1	2	3	4	5
I see myself as someone who tends to find fault with others	1	2	3	4	5
I see myself as someone who does a thorough job	1	2	3	4	5
I see myself as someone who gets nervous easily	1	2	3	4	5
I see myself as someone who had an active imagination	1	2	3	4	5

6. (AW) To what extent you agree with the following statements?

1 = Strongly disagree, 2 = Disagree, 3 = Neither agree or disagree,4 = Agree, 5 = Strongly agree					
I am aware of the privacy issues and practices in our society.	1	2	3	4	5
I follow the news and developments about the privacy issues and privacy violations.	1	2	3	4	5
I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy.	1	2	3	4	5
Web sites seeking information online should disclose the way the data are collected, processed and used.	1	2	3	4	5
A good online privacy policy should have a clear and conspicuous disclosure.	1	2	3	4	5

7. (V) To what extent the following ideas represent a life-guiding principle for you personally?

1 = Absolutely no, 2 = No, 3 = Neither yes, neither no, 4 = Yes, 5 = Absolutely yes					
Power, that is, social power, authority, wealth	1	2	3	4	5
Achievement, that is, success, capability, ambition, and influence on people and events	1	2	3	4	5
Hedonism, that is, gratification of desires, enjoyment in life, self-indulgence	1	2	3	4	5
Stimulation, that is, daring, a varied and challenging life, an exciting life	1	2	3	4	5
Self-Direction, that is, creativity, freedom, curiosity, independence, choosing one's own goals	1	2	3	4	5
Universalism, that is, broadmindedness, beauty of nature and arts, social justice, a world at peace, equality, wisdom, unity with nature, environmental protection	1	2	3	4	5
Benevolence, that is, helpfulness, honesty, forgiveness, loyalty, responsibility	1	2	3	4	5
Tradition, that is, respect for tradition, humbleness, accepting one's portion in life, devotion, modesty	1	2	3	4	5
Conformity, that is, obedience, honoring parents and elders, self-discipline, politeness	1	2	3	4	5
Security, that is, national security, family security, social order, cleanliness, reciprocation of favors	1	2	3	4	5

8. (ST1) How much do you trust…

1 = Absolutely no, 2 = No, 3 = Neither yes, neither no, 4 = Yes, 5 = Absolutely yes					
…strangers you meet for the first time	1	2	3	4	5
…public authorities	1	2	3	4	5
…police	1	2	3	4	5
…courts	1	2	3	4	5

9. (ST2) To what extent you agree with the following statements?

1 = Strongly disagree, 2 = Disagree, 3 = Neither agree or disagree,4 = Agree, 5 = Strongly agree					
In general, you can trust people.	1	2	3	4	5
When dealing with strangers, it's better to be cautious before trusting them	1	2	3	4	5

10. To what extent do you agree with the following statements?

1 = Strongly disagree, 2 = Disagree, 3 = Neither agree or disagree,4 = Agree, 5 = Strongly agree					
(BNF)					
In general, my need to obtain certain information or services from the Internet is greater than my concern about privacy.	1	2	3	4	5
I find that personal interest in the information that I want to obtain from the Internet overrides my concerns of possible risk or vulnerability that I may have regarding my privacy.	1	2	3	4	5
The greater my interest to obtain a certain information or service from the Internet, the more I tend to suppress my privacy concerns.	1	2	3	4	5
(NO)					
People should be able to use the Internet anonymously	1	2	3	4	5
People have the right to control personal information about themselves when online.	1	2	3	4	5
There should be no personal information gathering on the internet without consent.	1	2	3	4	5
(CA)					
Computers are a real threat to privacy in this country.	1	2	3	4	5
I am anxious and concerned about the pace of automation in the world.	1	2	3	4	5
I am easily frustrated by increased computerization in my life.	1	2	3	4	5
(OPC)					
I am concerned about my online privacy.	1	2	3	4	5
All things considered, the Internet would cause serious privacy problems.	1	2	3	4	5
Compared to others, I am more sensitive about the way my personal information is handled online.	1	2	3	4	5
I am concerned about extensive collection of my personal information over the Internet.	1	2	3	4	5
I am concerned about my privacy violation when using the internet.	1	2	3	4	5
Compared with other subjects on my mind, personal privacy online is very important.	1	2	3	4	5
(ATT)					
It doesn't bother me when websites track my online activities.	1	2	3	4	5
It doesn't bother me when websites ask me for personal information.	1	2	3	4	5
I'm concerned that websites are collecting too much personal information about me.	1	2	3	4	5
(CTRL)					
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.	1	2	3	4	5
My control of personal information lies at the heart of my privacy.	1	2	3	4	5
Personal information should not be used for any purpose unless it has been authorized by that person.	1	2	3	4	5
When people give personal information for some reason, it should never be used for any other reason.	1	2	3	4	5
(REG)					
The existing laws in my country are sufficient to protect peoples online privacy.	1	2	3	4	5
The government is doing enough to ensure that citizens are protected against online privacy violations.	1	2	3	4	5
There should be tougher regulations by the government to protect personal privacy online.	1	2	3	4	5
(SH)					
I don't mind sharing private pictures on the Internet.	1	2	3	4	5
I put private information on the Internet.	1	2	3	4	5
I don't mind posting on the Internet information about the place I am at the moment.	1	2	3	4	5
I don't mind posting on the Internet with whom I am at the moment.	1	2	3	4	5
I see no problem in sending my credit card data when buying online.	1	2	3	4	5

11. (PB) How often do you behave in the following ways when on the Internet?

1 = Never, 2 = Almost never, 3 = Sometimes, 4 =Almost every time, 5 = Every time					
I give fictitious responses to avoid giving the web site real information about myself.	1	2	3	4	5
I use another name or e-mail address when registering with certain web site without divulging my real identity.	1	2	3	4	5
When registering with certain web site, I only fill up data partially.	1	2	3	4	5
I use software so that the recipient cannot track the origin of my mail.	1	2	3	4	5
I use software to eliminate cookies that track my Internet activities.	1	2	3	4	5
I use software to disguise my identity.	1	2	3	4	5
I am reluctant to register with my personal information to the websites I don't completely trust.	1	2	3	4	5
I refuse to provide personal information to untrustworthy websites.	1	2	3	4	5
I avoid visiting the untrustworthy websites.	1	2	3	4	5
I don't purchase goods from untrustworthy websites.	1	2	3	4	5

12. (IT)

1 = Not interested at all, 2 = Not interested, 3 = Neither interested or not, 4 = Interested, 5 = Very interested					
How interested would you be in using new online services /technologies immediately after they're available?	1	2	3	4	5
1 = Extremely unlikely, 2 = Unlikely, 3 = Neutral, 4 = Likely, 5 = Extremely likely					
What is the likelihood that you will be one of the early users of new online services /technologies immediately after they are available?	1	2	3	4	5

13. (PE)

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

14. Have you ever bought goods or services on the Internet?

- Yes
- No

If YES, proceed with next question If NO, skip next question

15. How many times in last six months have you bought goods or services on the Internet?

_____

16. Gender M F

17. Age: _____

18. Education

- primary school or less
- secondary education
- tertiary education/high school, college, university
- master degree/doctoral title

19. How many people (including yourself) live in your household _____

20. Occupation

- Owner of the company / craft (own-account worker)
- Manager/official
- Professional (highly educated e.g. medical doctor, lawyer, bookkeeper, etc.).
- Technician/clerk
- Worker
- Retired
- Student
- Unemployed
- Other, please specify: _____

21. Total net average monthly income of your household

- ☐ up to 2.500 kn
- ☐ 2.501-5.000 kn
- ☐ 5.001-7.500 kn
- ☐ 7.501-10.000 kn
- ☐ 10.001-12.500 kn
- ☐ 12.501-15.000 kn
- ☐ more than 15.000 kn

22. County: _____

23. Settlement: _____

24. Size of your settlement (number of inhabitants)

- ☐ 10.000 or less
- ☐ 10.001-50.000
- ☐ 50.001-100.000
- ☐ more than 100.000

Interviewer: _____

Date: _____ Hour/minutes: _____

Phone number: _____

C. Questionnaire in Croatian

Poštovani, Ekonomski institut, Zagreb provodi istraživanje o stavovima građana o Internetu. Vaše sudjelovanje u istraživanju će nam biti od velike pomoći. Napominjemo da je istraživanje u potpunosti anonimno i da će se Vaši odgovori prikazivati isključivo skupno u tablicama koje će sadržavati postotke.

1. Koristite li se Internetom na bilo kojem uređaju? (npr. pametni telefon, računalo)
   - ☐ Da
   - ☐ Ne

(ako NE, kraj)

2. Procijenite koliko vremena u uobičajenom danu aktivno provedete na Internetu? (u satima) _____ sati

3. Za što sve koristite Internet?

Primanje i slanje e-mailova	Da	Ne
Korištenje chat/instant message servisa (npr. WhatsApp)	Da	Ne
Preuzimanje (download) glazbe i/ili filmova s Interneta	Da	Ne
Igranje online igrica	Da	Ne
Plaćanje računa/korištenje Internetskog bankarstva	Da	Ne
Pohađanje online kolegija ili tečaja	Da	Ne
Kupovina putem Interneta	Da	Ne
Slušanje radija putem Interneta (streaming)	Da	Ne
Gledanje videa putem Interneta (npr. YouTube)	Da	Ne
Telefoniranje putem Interneta (npr. Skype, Viber)	Da	Ne
Korištenje društvenih mreža (npr. Facebook, Twitter, Instagram)	Da	Ne
Praćenje dnevnih vijesti	Da	Ne
Traženje općih informacija na Internetu (npr. Google, Wikipedia)	Da	Ne
Aktivno sudjelovanje na online forumima (čitanje i pisanje postova)	Da	Ne
Korištenje servisa javne uprave putem Interneta (npr. prijave na natječaje, popunjavanje online obrazaca, online prijava poreza)	Da	Ne

4. Planirate li u budućnosti Internet koristiti u manjoj, podjednakoj ili u većoj mjeri nego do sada?

1 manje	2 podjednako	3 više

5. U kojoj mjeri sljedeća obilježja opisuju Vašu osobnost

1 = Uopće se ne slažem, 2 = Ne slažem se, 3 = Niti se slažem, niti se ne slažem, 4 = Slažem se, 5 = U potpunosti se slažem					
Smatram se rezerviranom osobom	1	2	3	4	5
Smatram se osobom koja ima povjerenja u druge ljude	1	2	3	4	5
Smatram se lijenom osobom	1	2	3	4	5
Smatram se opuštenom osobom koja dobro podnosi stres	1	2	3	4	5
Smatram se osobom zainteresiranom za umjetnost	1	2	3	4	5
Smatram se društvenom osobom	1	2	3	4	5
Smatram se osobom koja prebacuje krivnju na druge	1	2	3	4	5
Smatram se temeljitom osobom	1	2	3	4	5
Smatram se nervoznom osobom	1	2	3	4	5
Smatram se osobom bujne mašte	1	2	3	4	5

6. U kojoj mjeri sljedeće ideje predstavljaju Vaša osobna životna načela?

1 = Uopće ne, 2 = Ne, 3 = Niti da, niti ne, 4 = Da, 5 = U potpunosti da					
Autoritet, bogatstvo i društvena moć.	1	2	3	4	5
Uspjeh, sposobnost, ambicija, utjecaj na ljude i događaje.	1	2	3	4	5
Zadovoljavanje želja, uživanje u životu, udovoljavanje samom sebi.	1	2	3	4	5
Izazovan, raznolik i uzbudljiv život.	1	2	3	4	5
Kreativnost, sloboda, znatiželja, nezavisnost, biranje vlastitih ciljeva.	1	2	3	4	5
Otvorenost uma, ljepota prirode i umjetnosti, socijalna pravda, mir u svijetu, jednakost, mudrost, jedinstvo s prirodom, zaštita okoliša.	1	2	3	4	5
Pomaganje, poštenje, odanost, odgovornost, opraštanje.	1	2	3	4	5
Poštivanje tradicije, skromnost i poniznost, prihvaćanje svoje uloge u životu, posvećenost.	1	2	3	4	5
Poslušnost, poštovanje prema roditeljima i starijima, samo-disciplina, pristojnost.	1	2	3	4	5
Nacionalna sigurnost, sigurnost u obitelji, društveni poredak.	1	2	3	4	5

7. U kojoj mjeri vjerujete…

1 = Uopće ne, 2 = Ne, 3 = Niti da, niti ne, 4 = Da, 5 = U potpunosti da					
…nepoznatim osobama koje vidite prvi put	1	2	3	4	5
…tijelima javne vlasti	1	2	3	4	5
…policiji	1	2	3	4	5
…sudstvu	1	2	3	4	5

8. U kojoj mjeri se slažete sa sljedećim tvrdnjama?

1 = Uopće se ne slažem, 2 = Ne slažem se, 3 = Niti se slažem, niti se ne slažem, 4 = Slažem se, 5 = U potpunosti se slažem					
Svjestan sam problematike privatnosti u našem društvu.	1	2	3	4	5
Pratim zbivanja i vijesti o pitanjima privatnosti i njezinu kršenju.	1	2	3	4	5
Upoznat sam s pitanjima privatnosti i rješenjima koje poduzeća i Vlada uvode kako bi osigurali našu privatnost.	1	2	3	4	5
Web stranice koje zahtijevaju informacije na Internetu trebaju objaviti način na koji se podaci prikupljaju, obrađuju i koriste.	1	2	3	4	5
Kvalitetna politika zaštite online privatnosti treba biti jasno vidljiva.	1	2	3	4	5
Općenito, ljudima se može vjerovati	1	2	3	4	5
U slučaju nepoznatih osoba, bolje je biti oprezan prije no što im se ukaže povjerenje	1	2	3	4	5
Općenito, moja potreba za dobivanjem određenih informacija ili usluga s Interneta je veća od moje zabrinutosti za privatnost.	1	2	3	4	5
Moj je osobni interes za neku informaciju koju želim dobiti s Interneta jači od moje zabrinutosti za povredu privatnosti na Internetu.	1	2	3	4	5
Što su veći moji interesi za dobivanje informacija ili usluga s Interneta, to sam manje zabrinut za svoju privatnost.	1	2	3	4	5
Građani bi trebali biti u mogućnosti anonimno koristiti Internet.	1	2	3	4	5
Građani imaju pravo kontrolirati svoje osobne informacije kada su na Internetu.	1	2	3	4	5
Prikupljanje osobnih informacija na Internetu treba se provoditi samo uz pristanak te osobe.	1	2	3	4	5
Računala su ozbiljna prijetnja privatnosti u ovoj zemlji.	1	2	3	4	5
Zabrinut sam zbog tempa razvoja automatizacije u svijetu.	1	2	3	4	5
Lako se uzrujam radi povećane informatizacije u mojem životu.	1	2	3	4	5
Zabrinut sam za moju privatnost u online okruženju.	1	2	3	4	5
Uzevši sve u obzir, Internet bi mogao dovesti do ozbiljnih problema za privatnost.	1	2	3	4	5
U usporedbi s drugima, više sam osjetljiv/a oko načina na koji se na Internetu barata s mojim osobnim informacijama.	1	2	3	4	5
Brine me pretjerano prikupljanje mojih osobnih informacija na Internetu.	1	2	3	4	5
Brine me narušavanje moje privatnosti kada se služim Internetom.	1	2	3	4	5
U odnosu na druga pitanja o kojima vodim računa, osobna privatnost na Internetu mi je vrlo važna.	1	2	3	4	5
Ne smeta me kada web stranice snimaju/prate moje online aktivnosti.	1	2	3	4	5
Ne smeta me kad web stranice traže moje osobne informacije.	1	2	3	4	5
Brine me da web stranice prikupljaju previše mojih osobnih informacija.	1	2	3	4	5

Moja online privatnost podrazumijeva da imam autonomiju i kontrolu nad time kako će se informacije o meni prikupljati, koristiti i dijeliti.	1	2	3	4	5
Moja kontrola nad informacijama je ključna za moju privatnost.	1	2	3	4	5
Prikupljanje osobnih informacija na Internetu treba se provoditi samo uz pristanak osobe.	1	2	3	4	5
Kada ljudi iz nekog razloga daju osobne informacije, nikada ih se ne smije koristiti za neki drugi razlog.	1	2	3	4	5
Postojeći zakoni u Hrvatskoj su dovoljni da se zaštiti privatnost građana na Internetu.	1	2	3	4	5
Vlada u mojoj zemlji čini dovoljno da zaštiti građane od narušavanja online privatnosti.	1	2	3	4	5
Trebala bi postojati striktnija regulacija i propisi Vlade za zaštitu osobne privatnosti online.	1	2	3	4	5
Prihvatljivo mi je podijeliti privatne fotografije na Internetu.	1	2	3	4	5
Na Internet stavljam privatne informacije.	1	2	3	4	5
Prihvatljivo mi je na Internetu objaviti gdje se trenutno nalazim.	1	2	3	4	5
Prihvatljivo mi je na Internetu objaviti s kime trenutno provodim vrijeme.	1	2	3	4	5
Prihvatljivo mi je poslati podatke s moje kreditne kartice kad kupujem online.	1	2	3	4	5

9. Koliko često se na Internetu ponašate na sljedeće načine?

1 = Nikada, 2 = Gotovo nikada, 3 = Ponekad, 4 = Gotovo uvijek, 5 = Uvijek					
Dajem pogrešne odgovore kako bih izbjegao odavanje pravih informacija o sebi	1	2	3	4	5
Koristim drugo ime ili e-mail adresu pri registraciji na web-stranici bez otkrivanja svojeg pravog identiteta.	1	2	3	4	5
Prilikom registracije na neku web-stranicu, podatke ispunjavam samo djelomično.	1	2	3	4	5
Koristim software koji sprječava primatelja da prati porijeklo mog e-maila.	1	2	3	4	5
Koristim software koji eliminira kolačiće koji prate moje aktivnosti na Internetu.	1	2	3	4	5
Koristim software koji prikriva moj identitet.	1	2	3	4	5
Oklijevam se registrirati sa svojim osobnim informacijama na web stranice kojima ne vjerujem u potpunosti.	1	2	3	4	5
Odbijam otkriti osobne informacije nepouzdanim web stranicama.	1	2	3	4	5
Izbjegavam posjećivanje nepouzdanih web stranica.	1	2	3	4	5
Ne kupujem proizvode od nepouzdanih web stranica.	1	2	3	4	5

10. Koliko ste zainteresirani za korištenje novih online usluga ili tehnologija neposredno po njihovom uvođenju?

1 = U potpunosti nezainteresiran, 2 = Nezainteresiran, 3 = Niti zainteresiran, niti nezainteresiran, 4 = Zainteresiran, 5 = U potpunosti zainteresiran				
1	2	3	4	5

11. Kolika je vjerojatnost da ćete biti među prvim korisnicima novih online usluga ili tehnologija nakon njihovog uvođenja?

1 = Sigurno neću, 2 = Vjerojatno neću, 3 = Niti hoću, niti neću, 4 = Vjerojatno hoću, 5 = Sigurno hoću				
1	2	3	4	5

12. Jeste li Vi ili netko Vama blizak imali neugodna iskustva…

s povredom Vaše privatnosti na Internetu	Da	Ne
s povredom Vaše privatnosti općenito	Da	Ne

13. Jeste li ikada kupili proizvod ili uslugu putem Interneta?

- ☐ Da (nastaviti na iduće pitanje)
- ☐ Ne (preskočiti pitanje 18)

14. Koliko puta ste u posljednjih 6 mjeseci kupili proizvode ili usluge putem Interneta?

_____

15. Obrazovanje

- ☐ osnovna škola ili manje
- ☐ srednja škola
- ☐ viša škola ili fakultet
- ☐ poslijediplomski studij/doktorat

16. Spol M Ž

17. Dob: _____

18. Broj članova vašeg kućanstva _____

19. Zanimanje

- ☐ Vlasnik poduzeća ili obrta
- ☐ Rukovoditelj (manager)
- ☐ Stručnjak (VSS ili više npr. liječnik, odvjetnik, računovođa)
- ☐ Službenik (radi uglavnom u uredu)
- ☐ Radnik
- ☐ Umirovljenik
- ☐ Student/učenik
- ☐ Nezaposlen
- ☐ Neko drugo zanimanje, koje? _____

20. Ukupna mjesečna primanja vašeg kućanstva

- ☐ Do 2.500 kn
- ☐ 2.501-5.000 kn
- ☐ 5.001-7.500 kn
- ☐ 7.501-10.000 kn
- ☐ 10.001-12.500 kn
- ☐ 12.501-15.000 kn
- ☐ više od 15.000 kn

21. Županija: _____

22. Mjesto: _____

23. Veličina mjesta po broju stanovnika

- ☐ 10.000 ili manje
- ☐ 10.001-50.000
- ☐ 50.001-100.000
- ☐ više od 100.000

Anketar: _____

Datum: _____ Sat/min: _____

Broj telefona: _____

ISBN 978-953-6030-50-7

e-ISBN 978-953-6030-50-7