PARADOX OR CYNICISM: THE QUESTION OF PRIVACY CONSIDERATION IN MOBILE APP USE

Hrastović, Dina

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, The Faculty of Political Science / Sveučilište u Zagrebu, Fakultet političkih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:114:956254

University of Zagreb

Faculty of political sciences

MSc Journalism

Dina Hrastović

PARADOX OR CYNICISM: THE QUESTION OF PRIVACY CONSIDERATION IN MOBILE APP USE

MASTERS THESIS

Zagreb, 2021

University of Zagreb

Faculty of political sciences

MSc Journalism

PARADOX OR CYNICISM: THE QUESTION OF PRIVACY CONSIDERATION IN MOBILE APP USE

MASTERS THESIS

Mentor: doc. dr. sc. Antonija Čuvalo

Student: Dina Hrastović

Zagreb

September 2021

I hereby declare that I wrote my dissertation **Paradox or cynicism: the question of privacy consideration in mobile app use**, which I submitted for evaluation to my mentor doc. dr. sc. Antonija Čuvalo, independently and that it is entirely my own work. Also, I declare that the work in question was not published or used for the purpose of fulfilling teaching obligations at this or any other university, and that I did not gain ECTS credits based on it.

Furthermore, I declare that in my work I have respected the ethical rules of scientific and academic work, and especially Articles 16-19. Code of Ethics of the University of Zagreb.

Dina Hrastović

Table of Contents

Table of Figures

Introduction

The question of personal privacy online is becoming ever so important due to the rising number of questions surrounding it in contemporary public discourse. Issues surrounding the conduct of a number of leading social and digital platforms on the global market are being discussed almost daily in international newspapers and political and academic circles. The controversy of data commodification – turning data on private users of online services in marketable goods – is not questioned anymore, but how the society should confront it at large.

A surge of interest in user behavior, one's privacy and digital literacy and awareness of these issues, has become one of the symptoms of this process. Although still very young, a growth of research on individual behavior online and disclosure of personal information has been remarkable in recent years. A leading phenomenon that prompts ever more interest in the topic is the incoherence between users' concerns and attitudes towards personal privacy online and their behavior in sharing personal information, which has been name the privacy paradox (Brown, 2001; Acquisti and Gross, 2006). Namely, the basis of the paradox lays in the incongruity of this observation with the leading psychological theory of human behavior. According to the theory of planned behavior, one is to behave in a way that one has the intention to behave, and this intention is based upon the assessed risk and one's attitudes towards the behavior. Numerous other concepts have in the meantime been tested as more or less relevant predictors of one's behavior, yet they have always remained a puzzle in the theory of planned behavior.

The exploration of privacy paradox, thus, followed suit. Most of the research, as discussed in this paper, focused on previously established antecedents of human behavior. Still, no good explanation to the privacy paradox has been offered, but to dismiss it entirely. Recent meta-analysis (Kolokakis, 2019) has shown little to no compelling evidence as to why despite rising concerns about their own personal privacy online, users still share their data generously.

By some critical thinkers, such an overwhelming focus on the individual behavior is a wrong approach to the issue in itself. They have criticized it as framing an international and institutional issue as a responsibility of an individual. Placing the blame, one might argue, on a layman that has little to no choice, while the finger should be pointed on the system at large. Smyrnaios (2018) and Fuchs (2011) discuss the process of commodification of users' data as a blunt exploitation of audiences by new digital media. It is the discourse of personal responsibility in one's online

conduct together with the frame of public communication in online social platforms, Fuchs argues, that shapes the way we approach the definition of the issue and possible solutions to it.

Along similar lines, a novel concept of privacy cynicism (Hoffman et al., 2016) has been proposed as to shine light on the greater scheme of contemporary societal processes concerning online marketplace. Privacy cynicism builds upon the previously established literature on cynicism and is defined as resignation, mistrust, uncertainty, and powerlessness of users to contribute to the state of their own personal information online due to present market and legal processes.

The aim of this study is to examine privacy cynicisms as a possible answer to the privacy paradox. In the next section, the theoretical background of privacy concerns online, the privacy paradox and cynicism is discussed in detail. In the following section, the research design and methods are presented. The following are the results of hypotheses testing. The paper ends with a discussion and further considerations.

Theoretical background

Personal privacy.

Privacy as "the right to be let alone" was an idea first introduced by Samuel Warren and Louis Brandeis in the 1890 article *The Right to Privacy.* It proposed the idea that an entity's right or need of certain information always has to be weighed against the individual's right or need of privacy (Lippert & Swiercz, 2007, p.17). This premise became the founding text for the development of privacy law in western world (ibid). Personal privacy as a set of procedures protecting our personal data from exploitation has since recently escalated among the top global issues of the newly digital economy.

> All these tracking methods result in markets where gigantic quantities of information on the profiles and habits of internet users are exchanged and sold continuously by specialised companies. Most of these firms are unknown to the general public, such as BlueKai, which has a database of one billion consumer profiles each with about fifty attributes, and Datalogix, which holds information on past business transactions valued at $2trillion. (Smyrnaios, 2018, p. 191)

In *Internet Oligopoly,* Smyrnaios (2018) addresses the issues of online user tracking and immense user data generation and trading as part of the undeniable oligarch play at stake. The author argues

the society has already reached a point at which users have little to no control in how their data is gathered, processed and shared with other parties – namely, companies as clients – and the development of further more connected and intrusive gadgets and services will only continue to do so even more. In similar vein, a global study conducted by Razaghpanah et al. (2018) revealed 2.121 tracking service online and explored their business conduct against the most recently introduced privacy policies, such as GDPR. According to their analysis, sharing user data among the tracking service providers is a norm of business conduct in the industry, with more than 80 percent of analyzed "mobile apps reserving the right to share tracking data with third-parties" (p. 12). The authors warn that despite the progress of enforcing novel privacy policies, they all fall short in three major areas. Firstly, due to the opacity of these systems, it is difficult to confidently track the sourcing, processing, and distribution of user data. Secondly, the introduced policies leave too much room for interpretation in terms of how the user consent should be obtained. Thirdly, these policies "do little to limit the sharing and selling of data by these organizations, leaving users with almost no control of who has access to their data" (Razaghpanah et al., 2012, p. 12).

The highlighted lack of control and power of users in these processes and a market ecosystem as a whole, has become a steppingstone for the introduction of critical theory to the issue, namely the contestation of privacy and surveillance. There are two established critiques that build on each other and are presented in the following paragraphs.

One line of economic critique of user data and their lack in controlling it builds on the value of privacy. Fuchs (2014) maintains that the contemporary notion of privacy is a rather ideologically charged construct of value that derives from John Stuart Mill's notion of economic privacy and the capitalist notion of private individuals making choices for their own private interests (p. 140). In other words, Fuchs holds that instead of blindly protecting privacy, we should firstly question the construct of privacy and whom in our society it benefits the most. In an intriguing article named *Towards an alternative concept of privacy,* Fuchs (2011) builds on an abundance of criticism arguing that the concept of privacy as it is now "promotes an individual agenda and possessive individualism that can harm the public/common good", "be used for legitimizing domestic violence in families", "be used for planning and carrying out illegal or antisocial activities",

"conceal information in order to mislead and misrepresent the character of individuals and is therefore deceptive", and "that a separation of public and private life is problematic" (p. 224).

Yet a far richer tradition of exploring and discussing privacy focuses on the positive values of protecting it (Solove, 2008; Schoeman, 1984). These are countered by Fuchs as unhistorical accounts that portray privacy as a universalistic truth and are therefore, according to the Marxist tradition, fetishistic thinking – "phenomena that are created by humans and have social and historical character [mistaken] as being natural and existing always and forever in all societies" (Fuchs, 2011, p. 226). The importance of this argument lays in its implications for modern society. Privacy as a societal norm and as a category of information not discussed publicly, indeed protects contemporary building blocks of western societies – private property. As long it is not discussed, it cannot be criticized (Fuchs, 2011, p. 230).

Another line of critique has foremost relied on the notion of digital labor. Smyrnaios (2018) writes

> Today, simply being online is enough to generate a huge quantity of data that users have no control over and that are used commercially. This is a paradigmatic form of digital labor, that is, an activity that reduces our digital interactions to a moment in the relations of production and signals that the social world is being subsumed to the merchant world in our users of technology. (p. 130)

Dallas Smythe's work is considered to make the foundation of audience labor and their data commodification (Fuchs, 2014). Smythe's arguments set off with a critique of radio and television commercialization which consequently implied selling viewership. Thus, the transaction of services for content sponsorships and advertisements was not over until a viewer would visit a store and buy the marketed good or service. Smythe warned how audience indeed has power, yet it is neither distributed nor commercialized by them, but by media – those of more capital and even more power (Fuchs, 2014, p. 86). Here, Fuchs builds on his argument for the question of digital media and online social networks. Namely, he points out that "the means of communication that Facebook and Twitter provide to its users are not a simple means of survival and should not be analytically treated as such, but a rather also means of production for the creation of value and profit" (p. 89) and introduced the notion of prosumer commodity – commodified consumers who are producers of value in online social networks (p. 93). Fuchs (2012; also see Fuchs, 2009) criticizes the mainstream academic approach to the issue of personal privacy and social networking

sites as it puts forward the responsibility of users on an individual level to disclose their information rather than a question of societal moral:

> They conceive privacy strictly as an individual phenomenon that can be protected if users behave in the correct way and do not disclose too much information. The moralistic tone in these studies ignores how Facebook commodifies data and exploits users as well as the societal needs and desires underpinning information sharing on Facebook. (p. 142)

So far, there have been fine distinctions between labor and play, on the one hand, and public and private on the other. These distinctions made up a strategic framework for the stability of capitalism (Fulcher, 2015; Arendt 1958). For as long as workers had their leisure time, their work discipline shall not be interrupted. For as long as workers perceived their out-of-work affairs as their own property, they shall not interfere with that of their employer. However, Fuchs notices that time of fine lines has come to an end and it is the disruption of this deceptive stability that now offers yet another economic shift in favor of capitalists:

> Facebook is a typical manifestation of a stage of capitalism in which the relation of the public and the private as well as labor and play collapse, and in which capital exploits this collapse. On Facebook, the corporation collects all private data and user behavior and commodifies both, while hiding these processes from the users. So the main form of privacy on Facebook is the opacity of capital's use of personal user data based on its private appropriation. (p. 147)

Rather than conflicting, these two criticized aspects of online economy build on each other, providing further accumulation of capital by those who already own the most. Private user data is commodified by a business using a convenient argument of public communication in order to increase the private capital of that same business. Economic surveillance via social media platforms has become a norm of surveilling primarily individual users and accumulating information, later translated into competitive knowledge of business, with the purpose of advancing their own market efforts (Fuchs, 2014). Users “dynamically and permanently create and share user generated content; browse profiles and data; interact with others; join, create and build communities, and co-create information”, whereas “the corporate web platform operators and their third party advertising clients continuously monitor and record personal data and online activities, […] store, merge and analyze collected data” (p. 100) that allows them to create detailed user

profiles of interests and behaviors and can further be monetized in personalized and targeted advertising.

The issue of personal privacy, especially of user-generated data in online platforms and applications, are often discussed in terms of individual behavior, as the rest of this paper will show. However, the moral of the critical approach to the privacy related issues of online behavior raise important questions like how the discourse around privacy issues might be framed, how it has changed and who exactly it benefits or harms. These questions are academically and societally immensely important in order to answer the most vital challenges of social change prompted by the immersion of new and connected technologies in everyday lives of citizens around the world.

Privacy paradox.

The sudden rise of exemplary events of personal data fragility online and the growing body of voices about privacy issues in public discourse have led to an unexpected turn of events among internet users. A growing body of research shows that individual's concerns and attitudes about online privacy do not reflect in their behavior, which is a ground argument of an established psychological theory – the theory of planned behavior. According to the theory, it is our attitudes, subjective norms and perceived behavior control that make up our intention and behavior in a certain way (Ajzen, 1991). It is of common understanding, thus, that our attitudes and beliefs translate into intentions and finally actions. However, the phenomenon in question has so far been confirmed in numerous areas of online behavior rather as a rule of online behavior than an exception to almost an axiom in psychology.

A qualitative research published two decades ago recognized the privacy paradox during the first rise of internet shopping and loyalty cards. Brown (2001) conducted interviews with 12 diverse participants in their gender, internet shopping experience, occupation, and age. These interviews pointed out how the experience of shopping online was marked by ever-present concerns about their privacy and data collection. The author marks how regardless of the experience in and the frequency of internet shopping, participants continue to share the same concerns about privacy as those of less experience. One of the participants shared

> Yes, someone might steal my details or what proof have I got, I haven't physically got a ticket in my hand, I haven't physically got a receipt in my hand, what is there to saw when

> I get to the airport my tickets don't arrive, […] But having said that I do book my flights over the internet because it's cheaper. (Brown, 2001, p. 16)

Along the similar lines, Acquisti and Gross (2006) examined the link between privacy concerns of individuals and their propensity to join online social networks at the early stages of Facebook, MySpace and Frindster. The authors report, according to survey answers by 147 American participants, how privacy concerns do not have an effect on whether one will join an online social network. Moreover, they show how more often than not, participants express dichotomies in privacy concerns and their actual behavior. Norberg and colleagues (2007) tried to explain the phenomenon by adapting the aforementioned model of planned behavior. Instead of having risk and trust as immediate antecedents of behavioral intention and mediated antecedents of behavior itself, they propose a model in which neither the intention leads to behavior, but also trust is rather an antecedent of behavior and not the intention to behave (p. 104). Their study indeed shows once again that "the level of actual disclosure significantly exceeded individuals' intentions to disclose" (p. 118) and conclude that behavioral intentions cannot be taken as an accurate predictor of behavior in the realm of privacy.

Over time three approaches to exploring the privacy paradox have emerged. Firstly, numerous academics developed an economic model and supported the thesis called the privacy calculus. The thesis posed that individuals take into consideration contextual information in order to assess the risk and the benefit of sharing information and make a decision to share accordingly. Secondly, risk awareness, or rather lack thereof, was addressed as a possible explanation to the gap between individuals concerns and actual behavior. If people were concerned, but not really aware of risks at stake, their behavior would lack grounds to change from current habits. Finally, the role of trust was assessed as a psychological factor that plays an important role in other cognitive and emotional processes. According to this approach, trust in the online environment or a specific online business could subsidy the lack of security we perceive or feel while using a service. Selected research conducted according to the three approaches is reviewed in the remainder of the section.

Approaching the privacy paradox issue from an economic point of view, seeing people as rational decision makers supporting their own self-interests, was already proposed by Brown (2001) once he presented his observations. Despite the concerns which represent the individual's assessment of risk, the gain of conducting an online transaction is greater than possible loss (p. 16). The

rational approach was further explored by a number of researchers which has led to a more prominent role of the privacy calculus. Lee et al. (2013) explored the extent to which both risk and benefits fit the predictive model of privacy disclosure behavior and found that both independent variables have a strong effect on behavior, yet benefits seemed to outperform the risks. Moreover, their model with both variables outperformed the two statistical model with single predictors.

Li et al. (2011) explored a step before the risk-benefit analysis and investigated the role of emotions and fairness levers on the decision-making process. They found that the two predictors play a role in forming the privacy protection belief and the privacy risk belief which led to the behavioral intention. Along similar line, Xu et al. (2011) supported the role of institutional structures and privacy assurance on individual's perception of risk and control in order to increase one's intent to disclose personal information. However, as discussed earlier, the intention has lack of validity according to numerous other studies in predicting actual online privacy behavior.

Norberg et al. (2007), as mentioned earlier, proposed a different model to behavior placing the spotlight on trust as the primary antecedent of behavior, rather than intention or risk. An analysis of data generated by an industry-oriented survey among 1000 U.S. citizens, inspected the role of procedural fairness, as a way of building trust among company's users, and users' willingness to disclose personal information (Culnan & Armstrong, 1999). The authors concluded "that procedural fairness can successfully address privacy concerns, and when fair information practices are observed, customers will be more willing to continue in the relationship with the firm" (p. 112). Nonetheless, the growing body of supporting evidence for the privacy calculus has been confronted with the limitations of the rational approach – namely, the psychological limitations of humans to access and process all relevant information to make an arguably rational decision known as the bounded rationality argument (Kehr et al., 2015; Wilson & Valaich, 2012; Keith et al., 2012; Acquisti & Grossklags, 2009).

As an answer to the disruption of the model, but still in line with the privacy calculus thesis, Dinev and Hart (2006) proposed an extended privacy calculus model by adding trust as an affective and key variable in the process. Rather than a predictor together with perceived risk, the authors propose trust as a mediating variable between risk and behavior and prove a great deal of influence trust has over privacy behavior. McCole and colleagues (2010) turned the model around and examined three common trust consideration – vendor trust, internet trust and third parties' trust –

in attitudes towards online purchasing and the moderating role of privacy and security concerns. They found trust in vendor was more important and trust in internet was lesser when a participant had higher privacy and security concerns (p. 1022-1023). An empirical evaluation of trust in social networking platforms was proposed by Krasnova et al. (2010). Via an online survey, the authors obtained answers by 259 participants in Germany. The results of the study once more support the role of risk in one's willingness to disclose their personal information, yet also shows that trust in the platform rather than other users can significantly adjust the perceived risk (p. 121-122).

Finally, the question of user's risk-awareness was raised in the privacy behavior model. Can risk-awareness, or lack thereof, impact one's decision making in terms of disclosing personal data online? Bartsch and Deinlin (2016) thought so and conducted an online survey with 630 Facebook users. The study showed that people who spent more time on Facebook and those who have changed their privacy settings more frequently, also had higher online privacy literacy. Further, those of higher privacy literacy were felt more secure and applied more social privacy settings. This is an important finding since earlier large-scale survey have indicated that people, younger generations especially, have false beliefs about their security online and the jurisdiction of national legal entities to protect their personal information (Hoofnagle et al., 2012). Trepte and colleagues (2015) went as far to propose an Online Privacy Literacy Scale (OPLIS) as a way to address the issue according to the knowledge fap hypothesis which posits that the lack of privacy literacy prevents users to react despite their concerns and wish to behave accordingly. Hargittai et al. (2010) investigated the same issue in a longitudinal study among more than 1000 bachelor students in the U.S., which showed that once induced, privacy literacy can be learned and affect one's online privacy behavior. Furthermore, the same study confirmed privacy literacy is just one of many issues affected by economic and social class struggles, as mostly those students with parents of higher education, white and Asian American, and male scored better in online privacy literacy.

Limitations of addressing the privacy paradox, as it has been until now, is being questioned by a rising number of scholars. Kolokakis (2017) conducted the most comprehensive meta-analysis of the available research on the privacy paradox and concluded that the discrepancy in attitudes and behavior we have named privacy paradox undeniably exists. However, the author argues how all offered models, which we previously discussed, offer unstable and weak effects to defend one or all as reasonable explanations of human online behavior. In this fashion, after applying as many

model constructs as they can, Dienlin and Trepte (2015) conducted one of the broadest scientific tests of the privacy paradox via questionnaire answers from 595 participants. Once all hypothesized connections were put together, the authors discovered that privacy paradox disappears once there is a fine distinction between privacy attitudes and privacy concerns.

Another limitation, I argue, is the lack of literature concerning the privacy paradox among smartphone users. The use of mobile phones versus desktop for activities online has been steady growing for years. According to the latest statistics, visits of online content via mobile phones have reached 68 percent compared to 29 percent done using a desktop browser in 2020 (Perficient, 2021). According to Statista (2021), the number of smartphone users has reached 3.8 billion in 2020, which is a twofold increase in the past 5 years. Together with the increase in the use of smartphones, the use of mobile apps grows accordingly. In 2020, about 208 billion downloads took place, not counting re-installations and updates (Statista, 2021).

The body of research devoted to examining privacy considerations and actual behavior among mobile users is, however, noticeably limited. Present research shows patterns similar to those discussed above yet finds some more specific norms of behavior characteristic for smartphones. For example, Kelley et al. (2013) found that users value more cost, functionality, design, rating, reviews and downloads when deciding whether or not to download a mobile app, rather than privacy settings or third-party policies. Sunyaev et al. (2015) addressed the issue of ranking apps in app stores as an antecedent to an app being downloaded rather than user privacy considerations. Namely, they explored the effect of rating and number of downloads as the main ranking factors, which when more positive or of higher number afford the app a higher ranking and consequently higher visibility in the app store. Along similar lines Barth et al. (2019) went to explore the possible influence of one's technical knowledge, privacy awareness and financial literacy on the app purchase decision-making. Under the premise of evaluating apps for what they are as a product, 39 students of technical educational background took part in the study. Even in the case of high control for differences between the apps and with participants of higher-than-average digital literacy, price, rating and design played a more important role in deciding whether to download (or purchase) and app or not. Moreover, despite reporting high importance of security permissions while downloading an app, in the following phases of the study participants' behavior was not in accordance with the earlier statements they had made. Authors point out that the same patterns

were observed in earlier research when the use of location-based applications was examined (Zafeiropoulou et al., 2013).

To summarize, users of online services show a discrepancy in their concerns towards and actual behavior of personal privacy disclosure. This phenomenon deviates from the established theory of planned behavior according to which attitudes together with risk and control predict one's behavioral intention and behavior consequently. There are three academic lines of investigation that have developed so far. A great body of research had examined the role of rational cost-benefit analysis, trust and lack of risk-awareness in one's decision-making process ahead of disclosing personal information online. However, once all variables from different models were put together, the issue of not distinguishing privacy attitudes from privacy concerns was uncovered. Another problem arises in the growth of smartphone use around the world, which is at the same time more diverse in functions and more intrusive in terms of privacy for their users. The body of research that has addressed the privacy paradox among mobile app users illustrates this issue. Mobile privacy behavior cannot be explained via the three proposed metrics as recent studies have shown app characteristics such as their placement in an app store and their design play a greater role in deciding whether to install them and use them, even for highly technologically and privacy literate users.

Privacy cynicism.

In view of the findings by Dienlin and Trepte (2015), Hoffman et al. (2016) proposed a completely different approach to exploring online privacy behavior and introduced the term *privacy cynicism*. They define it as "an attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behavior subjectively futile" (p. 5). They utilize cynicism as a coping mechanism that allows us to face uncertainty and take on the perceived risk. It is driven by the acknowledgment of how powerless we are in a certain situation rather than finding a silver lining. Because of the rising mistrust in online platforms, just as the society has already experienced with traditional institutions, authors propose privacy cynicism as a model to explain our online behavior. In the study, Hoffman et al. conducted focus groups and online discussion groups with 124 participants hoping to detect the most prominent thoughts about online personal privacy among internet users and weather they address the criteria of uncertainty, powerlessness, and mistrust. In the study, number of participants referred to insecurity and uncertainty, powerlessness or loss of control, and mistrust, as predicted. Authors note that more

savvy internet users have as well expressed a dose of cynicism, despite their skills and knowledge. This finding is supported by the previously mentioned study of engineering students who despite their knowledge of privacy issues, did not take it into account when choosing mobile apps to use (Bart et al., 2019). Following this proposal, the same group of researchers that proposed the concept of privacy cynicism developed a scale to measure it and tested the model among 1008 online respondents in Germany (Lutz et al., 2020). Their results indicate each out of the four building blocks of cynicism plays its own role in the process. Their model together with resulting relationships is presented in Figure 1.

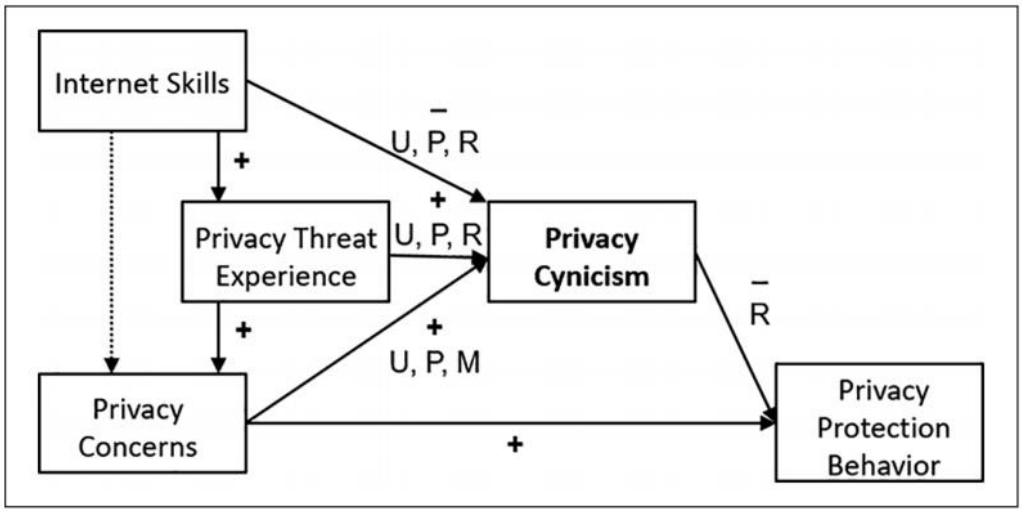


Figure 1. Summary of results in the model of privacy cynicism by Lutz et al. (2020)

In Figure 1, we can see that internet skills positively predict privacy threat experience which, in turn, contributes to privacy concerns. Internet skills also negatively affect uncertainty, powerlessness, and resignation as pillars of privacy cynicism. On the other hand, privacy threat experience positively contributes to the same categories of privacy cynicism. Privacy concerns also raise the feeling of uncertainty and powerlessness, but instead of resignation, they increase one's mistrust. Finally, predictive of privacy protection behavior in this model are only privacy concerns which increase the behavior, whereas out of the four pillars of privacy cynicism only resignation affect the behavior and negatively (p. 1181).

In their research, Hoffman, Lutz and Ranzini (2016; 2020), the authors of privacy cynicism, address its inevitable link to greater societal processes at stake. Going back to the question of privacy in contemporary society, they write how "convenience as well as fundamental relational

needs might lead individuals to feel trapped in the role of platform users" (p. 1182). In other words, the morale of exploring privacy cynicism is founded in its opportunity to explain how affections we have developed due to and towards mobile applications, and web services in general, are in the same time keeping as hooked despite our concerns and risks involved. Instead of questioning agency and will of users, it might be of more use to question the ecosystem altogether.

Research design

Due to a rise in smartphone use, it is of great importance to shed light on how we manage our privacy considering both current online privacy affairs and academic backing of the complexity of this issue. Thus, the aim of this study is to investigate the role of privacy cynicism among Croatian mobile app users as an alternative explanation to the privacy paradox.

In 2019, Ando Pavuna published his results in the empirical verification of privacy paradox in Croatia. Pavuna collected data via an online questionnaire and collected answers from 966 participants. The study supported the existence of privacy paradox, in as much as participants reported high privacy concerns and low criteria for giving up on their personal data online. The author notes that more than 90 percent of all participants declared privacy was of high or very high importance to them (p. 153). At the same time almost a third had not read a privacy policy of an app installed on their phone in past 6 months and less than a quarter did so rarely (p. 154). Pavuna ends by commenting on a small positive and significant correlation between privacy concerns and privacy behavior. Instead of predicting each other, the author remarks how there is some obvious interplay between the two variables, but the effect has not been established by this study. Pavuna adds how there is equal probability that in this case behaviors induce attitudes and not the other way around, which is a phenomenon known as 'cognitive dissonance'. According to this theory, people have hard time behaving differently from what they think and, therefore, may adjust their attitudes to be in line with their behavior, instead of the other way around.

In this research, I hope to offer a replication to the research by Pavuna (2019), introduce the concept of privacy cynicism and compare the models to clarify the interaction of the two models and their explanatory power over the issue of online privacy behavior among Croatian mobile app users.

The leading research question of this paper is *Can the discrepancy between privacy concerns and privacy behaviors known as a privacy paradox among mobile app users be explained by privacy*

cynicism? In order to answer this question, metrics of privacy cynicism should mediate the relationship between privacy concerns and privacy behavior, as in the model of Lutz et al. (2020), which I shall utilize here. With the intention to replicate the findings of Lutz et al. (2020) and confirm the viability of privacy cynicism among mobile users, the first hypothesis follows:

H1: Privacy cynicism mediates the influence of privacy concerns on privacy protection behavior.

Due to the findings of Dienlin and Trepte (2015), I shall add privacy attitudes as a distinct construct in the model and try to replicate their findings:

H2: Privacy concerns positively predict privacy attitudes.

The inclusion of privacy attitudes raises the question of their role in privacy cynicism. Attitudes together with risk and control are predictors of intention and later behavior, according to the theory of planned behavior. Whereas risk is an inherent characteristic of the act itself and one's calculation of probability of outcomes, the perceived behavioral control can be closely related to four elements of privacy cynicism: uncertainty, powerlessness, resignation, and mistrust. Furthermore, according to the model proposed by Hoffmann et al. (2016), privacy risk awareness is supposed to predict privacy cynicism rather than privacy behavior directly.

H3: Privacy risk awareness positively predicts privacy cynicism.

Given the confirmation of H3 or lack thereof, I will test whether privacy cynicism together with privacy attitudes and privacy risk awareness can better predict privacy protection behavior than any of the single linear models.

H4: Privacy cynicism and privacy attitudes better predict privacy protection behavior than any of the two alone.

Finally, due to aforementioned links between privacy literacy skills and the amount of time spent using internet or, in this case, mobile apps and the tested privacy behavior models, I introduce two more concepts to the model. Firstly, I will address the notion of privacy literacy which has previously been a significant predictor of privacy cynicism (Lutz et al., 2020), direct predictor of privacy behavior (Trepte et al., 2015; Bartsch & Dienlin, 2016) and was, in the same time, predicted by that same privacy behavior (Bartsch and Dienlin, 2016).

H5: Privacy literacy predicts privacy cynicism.

Furthermore, just the use of social networking sites has been shown as a predictor of privacy literacy (Bartsch and Dienlin, 2016). In this case such a relationship should exist between the use of mobile apps and mobile phones and privacy literacy of an individual.

H6: The use of mobile apps predicts privacy literacy.

H7: The use of mobile phones predicts privacy literacy.

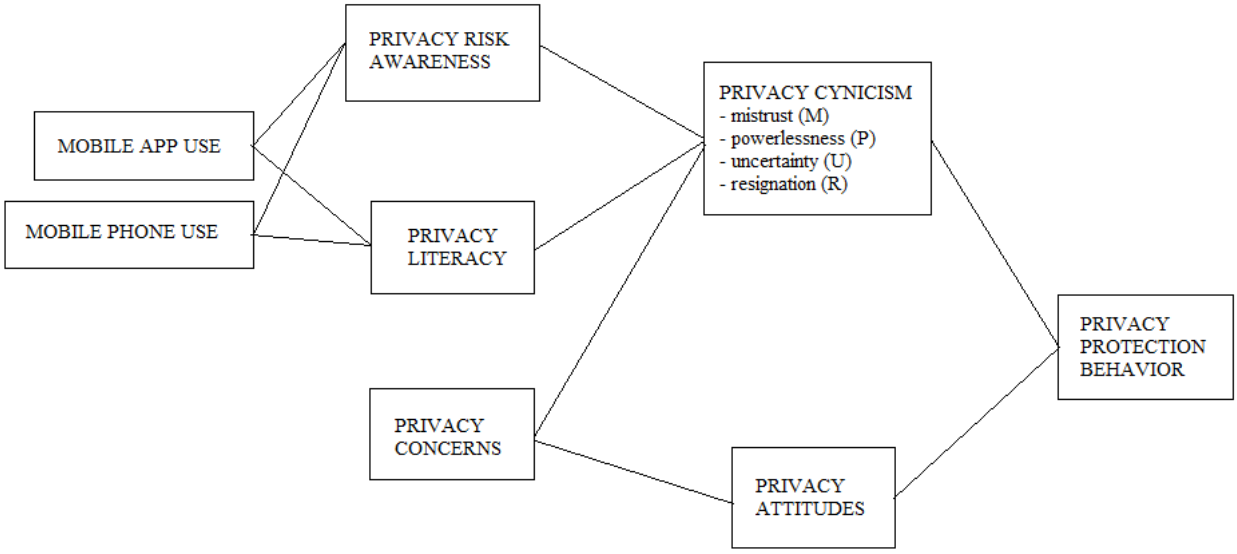
Given previous research has shown that the length of individual's internet use influences their familiarity with risks and consequently their privacy behavior, I postulate the use of mobile apps may positively predict the risk awareness which then mediates the relationship of use and privacy behavior.

H8: The use of mobile apps predicts privacy risk awareness.

H9: The use of mobile phones predicts privacy risk awareness.

In summary, I propose the following model, as portrayed in Figure 2, of privacy related behavior among mobile app users, which builds on the existing research on privacy paradox and is led by the novel privacy cynicism theory.

Figure 2. Research model



Methods

In order to test the proposed model, the research design of this study is a quantitative research based on a multi-linear regression model. I collected the data for the study via an online questionnaire distributed using social media platforms, Facebook primarily, and consisting of multiple scales established in previous research. I used Microsoft Excel and the XLSTAT add-in for the statistical analyses and hypotheses testing.

Questionnaire.

The online questionnaire consisted of three parts: (1) the demographics, (2) the use of mobile phones and apps, and (3) psychometrical scales. In the first part, participants were asked to share their age, gender, level of education and the size of their place of residence. In the second part, participants were asked to share their daily average of time spent using a phone and top 5 applications together with their respective average time of use. In the last part, participants were expected to consider the apps they just shared as their most used applications and answer whether they agree or not with statements making up nine different scales. The following table offers a neat overview of questions, whereas the entire questionnaire can be found in the Appendix 1.

PART 1 **Demographics**	General Inquiry	Age, gender, level of education, size of the place of residence
PART 2 **Mobile use behavior**	Behavioral measures	Average daily time use of mobile phone, average daily time use of top 5 most used apps
PART 3 **Psychometrics**	Privacy concern scale	Dienlin and Trepe, 2015
	Privacy literacy scale	Dienlin and Trepe, 2015
	Privacy protective behavior scale	Malik, 2016
	Privacy attitudes scale	Dienlin and Trepe, 2015
	Privacy cynicism scale	Lutz et al., 2020
	Perceived total risk and total benefit	Lee et al., 2013

Table 1. Used psychometric scales according to the questionnaire outline and academic source

The questionnaire was distributed over a three weeks long period from June 12, 2021 until July 1, 2021. As the author, I personally shared it via multiple public groups in Facebook. The same had been done by my coworkers and acquaintances.

Sample.

The final sample consisted of 101 participants. One case was dismissed due to insufficient data for analysis. The sample of 100 participants was finally analyzed for possible outliers using Grubbs test. No outliers were found.

Participants come from all age groups relevant to increased digital and smartphone use, ranging in age from 16 to 60 years old. The mean age is 31 years, whereas the median is 25, suggesting a primarily younger sample. Majority of participants were women making up 61 case, men 38 and there was one case of a nonbinary person. In terms of education, most participants

Exactly 80 percent of the sample live in a city with more than 100.000 inhabitants, eight percent live in a town with more than 10.000, four percent in a town with more than 2.000 and less than 10.000 inhabitants, and eight percent in a village with less than 2.000 inhabitants.

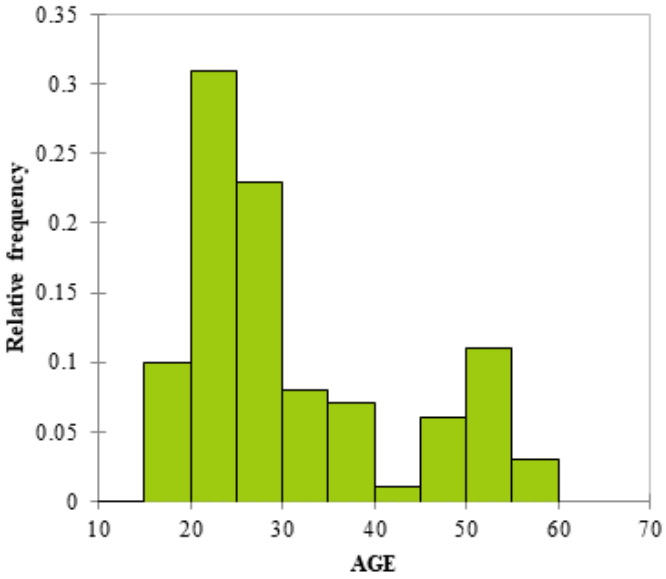


Figure 2. Histogram of samle age distribution

Condition analysis.

In this phase, I checked all the assumptions necessary before testing the hypotheses. Firstly, one of the questions regarding mobile and app use behavior considered whether participants would like to upload a screenshot of their scores in Digital Wellbeing phone feature, write the scores in the questionnaire themselves, or make an approximation of their mobile and app use on their own given they were not able to find the data in their phones in the time of taking the questionnaire.

Therefore, I tested the three groups of participants for possible statistical difference in their answers. I found no significant differences.

Secondly, I tested the scales used in the questionnaire for their scale reliability. The analyses showed the scales were highly reliable as presented in the Table X with each scale's Cronbach alpha score.

Scale		***Cronbach alpha (standardized)***
Privacy concern scale (PC)		0.913
Privacy literacy scale (PL)		0.845
Privacy protective behavior scale (PPB)		0.857
Privacy attitudes scale	Sharing data (PA_1)	0.642
	Protecting data (PA_2)	0.819
Privacy cynicism scale	Resignation (C_R)	0.895
	Powerlessness (C_P)	0.878
	Uncertainty (C_U)	0.875
	Mistrust (C_M)	0.899

Table 2. Summary of scales' reliability scores (Cronbach alpha)

Given all the scales were highly reliable, I made average scores per scale as the final variable for further analysis. Thus, the test of distribution normality followed. Each new variable representing already discussed scales was tested using the Shapiro-Wilks method. Out of eleven tested variables, two were indisputably normally distributed, six remained above the 0.001 threshold of statistical significance, and were most certainly not normally distributed. A detailed overview per tested variable is offered in Table X.

Scale	***Shapiro-Wilks***
PC_Avg	0.049*
PL_Avg	0.009*
PPB_Avg	0.052
PA_1_Avg	0.002*
PA_2_Avg	0.030*
C_R_Avg	0.151
C_P_Avg	0.008*

C_U_Avg	<0.001**
C_M_Avg	0.009*
Risk	<0.001**
Benefit	<0.001**

Table 3. Overview of scales' normal distribution (Shapiro-Wilks)
*[statistical significance: * for p <.05; ** for p<.01]*

The assumption of normal distribution was not met. Yet given the complexity of the topic and a relatively small sample of participants, this issue was to be expected.

Hypotheses testing results.

Once all the assumptions were checked, I proceeded to testing the proposed model. In total there are nine cause-effect relations assumed in this study, as presented earlier in the Figure X. I followed the hypotheses in the order of their presentation in the theoretical part of the study for this analysis.

H1: Privacy cynicism mediates the influence of privacy concerns on privacy protection behavior.

To test the above hypothesis, I firstly had to test the effect of privacy concern on both the privacy protection behavior and privacy cynicism separately. I used age as a control variable in both linear regressions. Privacy concern was not a predictor of privacy protection behavior. The test showed the model to be non-significant, F(2)=.104, p=.903.

As I decided to keep the scale of privacy cynicism as four separate features of the phenomenon, the test of the effect of privacy concern on privacy cynicism consisted of four models. The tests showed privacy concern does affect two out of four cynicism features. Namely, mistrust and resignation are not affected by privacy concerns, t(*mistrust*)=0.420, p=.676; t(*resignation*)=-0.096, p=.0923. Powerlessness and uncertainty were predicted by privacy concerns as follows t(*powerlessness*)=3.049, p(t)=.003; F(2)=6.766, p=.002; t(*uncertainty*)=5.084, p(t)<.001; F(2)=13.219, p<.001.

The summary of discussed results is presented in Table x. As privacy concern was not detected as a predictor of privacy protection behavior, there was no mediation to be tested. The hypothesis was not confirmed. Privacy cynicism does not mediate the effect of privacy concern on privacy protection behavior.

Still, I tested the effect of privacy cynicism on privacy protection behavior which is an integral assumption of the tested hypothesis. Out of the four features of privacy cynicism, one deemed a

statistically relevant effect on privacy protection behavior, which was resignation. Results are presented in Table 4.

Privacy protection behavior	***Standard error***	***t***	***p***
Intercept	0.418	9.535	<.001**
Cynicism – Mistrust	0.094	0.330	.742
Cynicism – Uncertainty	0.108	-1.503	.136
Cynicism – Powerlessness	0.103	-0.643	.522
Cynicism – Resignation	0.083	-4.219	<.001**
Age	0.006	1.743	.085

*Table 4. Linear regression model of privacy cynicism and privacy protection behavior [statistical significance: * for p <.05; ** for p<.01]*

H2: Privacy concerns positively predict privacy attitudes.

Age was once again the control variable in the linear model. The test showed privacy concern to predict privacy attitudes, yet only the part of the scale concerning attitudes towards sharing data (PA_1), and not the one concerning restricting online access to own data (PA_2). The linear model for the first part had the following results t=12.293, p=.024*; F(2)=2.674, p=.074. The second analysis the following t=-0.975, p=.332; F(2)=1.628, p=.202.

H3: Privacy risk awareness positively predicts privacy cynicism.

Privacy risk awareness in this study consists of two elements – the perceived risk and the perceived benefits of sharing data online. For the purpose of differentiating the two elements as they are not exclusive and opposites, they were left as separate variables in the analysis. Given there were four different models due to four features of privacy cynicism, with same predicting variables, a summarized overviews is offered in the Table 5.

	C-Mistrust		***C-Uncertainty***		***C-Powerlessness***		***C-Resignation***	
	t	*p*	*t*	*p*	*t*	*p*	*t*	*p*
Intercept	7.976	<.001**	9.455	<.001**	6.906	<.001**	5.163	<.001**
Risk	2.517	.013*	4.736	<.001**	4.688	<.001**	0.471	.638
Benefit	1.200	.233	-1.055	.294	-1.005	.317	0.196	.845
Age	0.211	.833	0.881	.381	2.294	.024*	2.297	.024*
R^2	0.070		0.212		0.234		0.056	

F	2.417	8.584	9.781	1.890
p(F)	.071	<.001**	<.001**	.136

*Table 5. Linear regression model of privacy risk, benefit and privacy cynicism [statistical significance: * for p <.05; ** for p<.01]*

As presented, risk as a part of privacy risk awareness is a predictor of three out of four features of cynicism: mistrust, uncertainty, and powerlessness.

H4: Privacy cynicism and privacy attitudes better predict privacy protection behavior than any of the two alone.

The fourth hypothesis largely leans on the abundance of published research of the effect of privacy attitudes on privacy protection behavior. However, in order to test, I had to first check whether the same is true in this study. The test showed there was no link causal relationship between either of privacy attitudes measures and the privacy protection behavior, t(PA_1) = 0.134, p = .894; t(PA_2) = 0.132, p = .997. Thus, the proposed hypothesis could not be tested, as the underlying assumption of causal effect of privacy attitudes was not confirmed.

H5: Privacy literacy predicts privacy cynicism.

The linear regression test, with age as the control variable, showed privacy literacy to be a predictor of privacy cynicism. More specifically, privacy literacy predicts uncertainty (t=0.095, p<.001), powerlessness (t=-2.801, p<.001), and resignation (t=-4.375, p<.001). Whereas people of higher literacy in privacy issues feel more uncertain, they feel less powerless and resignation from the issue less than those of lower privacy literacy. The summary of test results is presented in the Table 6.

	C-Mistrust		***C-Uncertainty***		***C-Powerlessness***		***C-Resignation***	
	t	*p*	*t*	*p*	*t*	*p*	*t*	*p*
Intercept	6.771	<.001**	11.160	<.001**	8.308	<.001**	7.906	<.001**
Privacy literacy	-0.473	.638	0.095	<.001**	-2.801	.006*	-4.375	<.001**
Age	0.151	.880	0.007	.539	0.999	.32	0.962	.338
R^2	0.003		0.143		0.110		0.209	
F	1.65		7.077		6.012		12.843	
p(F)	.848		.001**		.003*		<.001**	

Table 6. Linear regression model of privacy literacy and privacy cynicism
*[statistical significance: * for p <.05; ** for p<.01]*

H6: The use of mobile apps predicts privacy literacy.

H7: The use of mobile phones predicts privacy literacy.

According to the linear regression test, the use of mobile phone does not predict one's privacy literacy (t=0.761, p=.449), nor does the use of mobile apps (t=-1.035, p=.305). The hypotheses 6 and 7 were not confirmed.

H8: The use of mobile apps predicts privacy risk awareness.

H9: The use of mobile phones predicts privacy risk awareness.

The test of mobile apps and phones use in terms of predicting privacy risk awareness as described by two parameters, namely perceived benefit and perceived risk, showed there is no effect. The average time spent using a phone and using mobile apps does not predict perceived benefit (t(phone)=-0.886, p=.379; t(apps)=-1.819, p=.074) and does not predict perceived risk (t(phone)=0.435, p=.665; t(apps)=-0.944, p=.349). Hypotheses 8 and 9 were not confirmed.

Given all the hypotheses testing, all results of confirmed causal relationships is given in the following Figure 2.

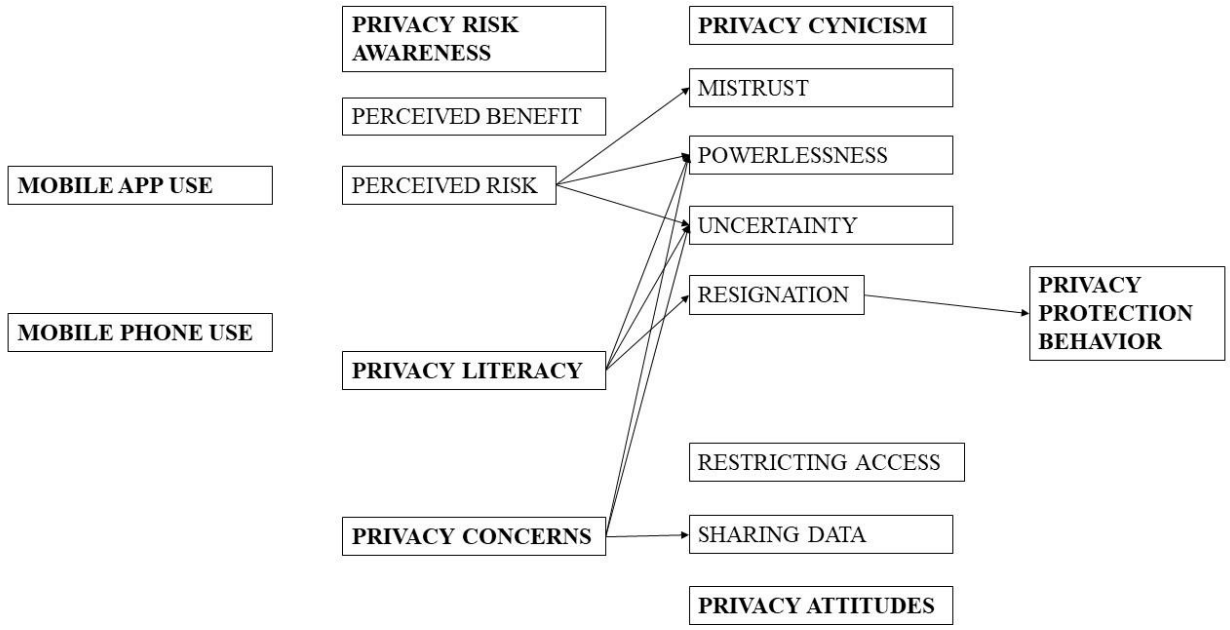


Figure 3. Research model confirmed causal relationships

In summary, this study shows how perceived risk, together with privacy literacy and privacy concerns influences one's privacy cynicism. Specifically, higher the perceived risk by users, higher is their mistrust, feeling of powerlessness and uncertainty. Privacy literacy has a negative effect on the feeling of powerlessness and resignation, but a positive effect on the feeling of uncertainty. Privacy concerns positively predict the feelings of powerlessness and uncertainty. Privacy concerns also predict privacy attitudes towards sharing personal data online in such a way that those of higher privacy concerns have more positive attitudes towards sharing personal data. Finally, out of all four features of privacy cynicism, only resignation negatively predicted privacy protection behavior.

Discussion

In the following section, I will contextualize the findings of this study, argue possible explanation of both confirmed and not confirmed relations between phenomena in question and consider both pitfalls and contributions of the present study in academia.

Findings.

The aim of this study was to investigate the role of privacy cynicism as a novel phenomenon and a scientific proposal in terms of the great privacy paradox. Privacy paradox is the behavioral

incoherence between users' concerns and attitudes towards personal privacy issues online and their willingness to adapt their behavior in sharing personal data. The study investigated this issue among Croatian mobile users and leaned on the previously published study of Pavuna (2019) which confirmed there indeed was a privacy paradox present among Croatian mobile phone users. Similarly, this study shows how, despite the strong ground upon which the theory of planned behavior lays, neither do privacy concerns nor privacy attitudes predict one's privacy behavior. Instead, as I anticipated in this study, privacy cynicism had a complex and important role in explaining users' privacy behavior.

Firstly, out of all predictors assumed from literature, it was only resignation as a feature of privacy cynicism that had a direct effect on privacy protection behavior. Those who had rather resigned from the issue of personal privacy online also exhibit less privacy protection behavior. One's resignation was measured using statements of senselessness to care about privacy issues, lack of resources to care about it properly or the feeling of making no difference by caring and doing something about it. According to the first study on privacy cynicism, and the only one know to me by the date of writing, conducted by Lutz et al. (2019), resignation is the only parameter of privacy cynicism confirmed and replicated in this study. In both cases, resignation has negatively predicted privacy protection behavior. The difference between the studies is the starting point of privacy cynicism investigation. Whereas Lutz and colleagues (2019) assumed individual differences between the four features of privacy cynicism, I assumed the causal relationship between them and privacy protection behavior. In that regard, my first hypothesis was not confirmed in as much as three out features had no effect on the privacy protection behavior and one had. In their study the hypothesis was measured not only against the existence of an effect, but the valence of it too. In other words, Lutz and colleagues expected to see a negative effect of all cynicism dimensions, yet only mistrust and resignation deemed a significant effect, and the effect of mistrust on privacy protection behavior was positive. In sum, this study replicates the finding of previous research on resignation, a spart of privacy cynicism, to negatively predict ones privacy protection behavior and, in such a way, play role in privacy paradox.

Secondly, contrary to some literature, including that of Lutz and colleagues, this study did not find an effect of privacy concerns on privacy protection behavior. There was also no effect found by privacy attitudes on privacy protection behavior. Rather, I found that privacy concerns do predict

the aspect of privacy attitudes concerning sharing personal data online, but not restricting access to it. Those of more emphasized privacy concerns, at the same time it seems, have a more positive outlook on sharing their personal data online. This is an interesting finding, not at least expected as it does not describe the relationship between a concern and attitude against a behavior, but between two cognitive processes and stances themselves. According to the theory of planned behavior, our behavior is not only highly correlated with out intentions due to the proximity of these processes, but because of human incompetence as well to make peace with an opinion that diverges from their actions, an incoherence in what one says and what one does. These findings, on the other hand imply there is no link between a fright we perceive and are conscious of and are attitude towards feeding that same fear. Thus, this study differs from the study of Lutz et al. (2019) yet replicates the findings of numerous others which in such a way supported the privacy paradox argument.

Thirdly, I investigated the role of privacy cynicism among the net of different psychological phenomena that has already been discussed as part of the privacy protection behavior model. Privacy risk awareness, privacy literacy and privacy concerns all had an influence over privacy cynicism, but of different kind and on different features of privacy cynicism. Perceived risk of sharing personal data online had a distinct positive effect on mistrust, uncertainty, and powerlessness of users. In a similar fashion, privacy concerns positively predicted uncertainty and powerlessness felt by users. However, only privacy literacy negatively predicted resignation in cynicism. In other word, those of higher privacy literacy tend to be less engaged around the issues of privacy and therefore, most probably given the results of this study yet standing unconfirmed, contribute to privacy protection behavior. The same was found by Lutz et al. (2019), yet their study also showed a negative link between literacy and uncertainty and powerlessness. Privacy concerns were also a predictor of cynicism parameters in their study, all positive relations but resignation which was negatively predicted. Yet, in this study privacy concerns' effect on cynicism is replicated only in terms of uncertainty and powerlessness.

Limitations.

There were some limitations to this study that must be acknowledged and discussed. These are mostly related to the methodological side of the study but do, at the same time, lay close to the theoretical framework. Namely, due to the recency of recognizing the issues of personal privacy online, there has been a sudden introduction of numerous established behavioral phenomena to the

topic in order to test all theoretically plausible explanations to privacy paradox. However, concurrent to this have been novel understandings of grater sociological processes such as the decreasing trust in established and traditional institutions, the ever-growing digital industry that resembles cartel-like market behavior and the transition in generations in terms of their familiarity to digital technology and online service. Although overwhelming and, one might argue, counterproductive in terms of scientific hypotheses testing, it would be ignorant to assume only one side to the issue as the leading explanation so early on the path towards understanding privacy paradox. Thus, a repeating issue in literature is the abundance of relationships and phenomena tested, which in this study has costed the analysis some more concrete conclusions.

Sample size is one of three factors in determining statistical power of an effect (Beck, 2013), together with the significance level and effect size. Now, to find an effect in an environment with predetermined significance level (usually .05 or .01) and a small sample size, the effect would have to be large. Whereas as for large samples, effect size can be small but still found and recognized as of great statistical power. In social science, smaller samples in statistical analysis weigh worse than larger ones, simply due to the nature of relationships and effects they explore. In such a way, the topic of privacy paradox and privacy cynicism is challenging to research as numerous phenomena are included and must remain there in order to question all assumption in detail as there is little tradition to rely on. On the other hand, it should be considered that the leading premise of privacy paradox is in its incoherence according to one of the leading behavioral theories. Yet, at the same time, it has been tested numerous times using the same phenomena and variables that the theory suggests.

Finally, although my belief from the start was that the issue of personal privacy online would be easier to grasp for participants in a general sense, instead of focusing on one mobile app, I now trust an issue arose from the multiversity of different apps participants could have been referring to as they filled in the questionnaire. To an extent, I tried to prevent it, via recurring reminders to think about all top 5 apps they had written in at the start of the questionnaire. Yet, the issue extends to the notion of top five apps as well due to some people, a minority but nevertheless, not finding these statistics in their phone and continuing with the questionnaire without a reference point. Some other, again a small part but still worth of mention, did not have top five apps in their digital wellbeing, but four or three.

Contribution.

The notion of privacy cynicism as an explanation for the incoherence in users' attitudes and behaviors in privacy is an important step in understanding the privacy paradox. Namely, the privacy paradox should not, especially at such an early stage, when there is still little understanding of it, be seen as a single feature of a single user. It is a sociological as much a psychological issue. A growing body of research is providing ever more evidence of people turning against the traditional ways of conducting business, forming trust, sharing information. To what an extent is this caused or mediated by the digital revolution is yet to be answered. But it is relevant to observe it as a whole and not as separate processes.

Privacy cynicism, although a measurement of individual attitudes, is a macro process in modern societies. Although it remains for further research to explore to what extent it applies and how big of a role it plays, cynicism has already been detected in numerous societal processes, especially voting and political engagement. The fact that only one variable out of four cynicism parameters predicted privacy protection behavior in this study and had at the same time less to do with the remainder of the model when compared to other parameters, already shows a different dynamic to the question of privacy paradox. It is the resignation that keeps people from acting upon their privacy attitudes and concerns. To what extent can an individual play a significant role in determining conduct around them or even who has access to what knowledge about them, is not a question to govern societies at this point but a question that governs individuals' choices everyday with or without their awareness. In such a way, cynicism as a critical approach in discussing contemporary behavioral issues has a prominent role and shines a completely new light on how we address psychological and sociological discrepancies.

Conclusion

In contemporary society the question of personal privacy is an ever-rising issues that is probed by an intensive datafication of human behavior online. Big amounts of data on patterns of behavior, attitudes, and demographics have made it easier than ever before to connect crucial dots in determining certain marketable features about online users that not even individuals themselves might be aware of. Yet, despite the growing awareness of business practices and data harvesting done by multiple leading digital companies in the world, online users seem not to behave in such a way as to protect their data from the ongoing exploitation. As this observation is also contrary to

a leading psychological theory of human behavior, the phenomenon has been named the privacy paradox. Although, observed by some in the past century already as an inexplainable issue with the invention of credit cards and online payments, it was not until recently that the issue got more academic attention.

Recent meta-analysis (Kolokakis, 2019) has shown, however, how inconclusive the consideration and research of the privacy paradox has been. Some have addressed this issue by questioning the basis of it being called a paradox, others have proposed a different approach. One of these novel approaches is the notion of privacy cynicism, developed and tested by Hoffman et al. (2016; see also Lutz et al., 2019). Privacy cynicism is a representative phenomenon of recent societal processes in terms of an increasing mistrust in establishment and the widespread feeling of powerlessness as an individual. The phenomenon is proposed by its authors as consisting of four distinct parameters that were developed from the existing literature on cynicism – mistrust, uncertainty, resignation, and powerlessness.

The aim of this study was to test this phenomenon among Croatian mobile app users, as there has already been proven the presence of the privacy paradox by an earlier study (Pavuna, 2019). The research model consisted of multiple upheld predictors of privacy protection behavior and privacy cynicism measurement. The analysis results indicate there is little to any relations between the often-used predictors of online privacy behavior and the behavior as such. For example, neither have privacy literacy, privacy concerns, nor privacy attitudes influenced privacy protection behavior. The only predictor of the examined behavior was one of the four privacy cynicism parameters – resignation. Whereas other cynicism parameters had a relationship with other assumed predictors of privacy behavior that were not confirmed by this study, resignation remained independent of the rest of the model. Most findings about privacy cynicism in the model supported the findings of Lutz et al. (2019).

Despite discussed methodological challenges of the study, there is an important takeaway from the introduction of privacy cynicism to the privacy research at large that should be considered. Modern society is going through immense behavioral changes. These processes are sometimes favored, sometime criticized, yet it remains for a fact that they influence the way one considers oneself as a unit in the society. Cynicism might be new in privacy research, yet it is a more prominent way of considering political, economic, and moral behavior in social sciences.

Literature

Acquisti, A., & Grossklags, J. (2012). An online survey experiment on ambiguity and privacy. *Communications & Strategies*, (88), 19-39.

Acquisti, A., & Gross, R. (2006, June). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies* (pp. 36-58). Springer, Berlin, Heidelberg.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Arendt, H. (2013). *The human condition*. University of Chicago Press.

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics*, *41*, 55-69.

Bartsch, M., & Dienlin, T. (2016). The study was conducted while Miriam Bartsch was student at the Institute for Psychology at University of Hamburg and Tobias Dienlin was research assistant at Hamburg Media School. 1–31.

Beck T. W. (2013). The importance of a priori sample size estimation in strength and conditioning research. *Journal of strength and conditioning research*, *27*(8), 2323–2337. https://doi.org/10.1519/JSC.0b013e318278eea0

Brown, B. (2001). Studying the Internet experience. *HP laboratories technical report HPL*, *49*.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80.

Flick, C. (2016). Informed consent and the Facebook emotional manipulation study. *Research Ethics*, *12*(1), 14-28.

Fuchs, C. (2014). Digital labour and Karl Marx. In Routlage (Issue 2). https://doi.org/10.4324/9781315768656-4

Fuchs, C. (2012). The political economy of privacy on facebook. Television and New Media, 13(2), 139–159. https://doi.org/10.1177/1527476411415699

Fuchs, C. (2011). Towards an alternative concept of privacy. Journal of Information, Communication and Ethics in Society, 9(4), 220–237. https://doi.org/10.1108/14779961111191039

Fulcher, J. (2015). *Capitalism: A very short introduction* (Vol. 108). Oxford University Press, USA.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2012). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1589864

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607-635.

Keith, M., Thompson, S., Hale, J., & Greer, C. (2012). Examining the rationality of location data disclosure through mobile devices.

Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013, April). Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 3393-3402).

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *PNAS*, *111*(24), 8788-8790.

Kücklich, J. (2005). FCJ-025 Precarious Playbour: Modders and the Digital Games Industry.

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of

balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, *71*(9), 862-877.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445.

Lippert, S. K., & Swiercz, P. M. (2007). Personal data collection via the internet: the role of privacy sensitivity and technology trust. *Journal of International Technology and Information Management*, *16*(1), 2.

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. New Media and Society, 22(7), 1168–1187. https://doi.org/10.1177/1461444820912544

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

McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, *63*(9-10), 1018-1024.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Pavuna, A. (2019). Privacy paradox: Empirical verification of the phenomenon. Politicka Misao, 56(1), 132–162. https://doi.org/10.20901/pm.56.1.05

Perficient. (March 2021). Mobile vs. Desktop Usage in 2020. Retrieved from https://www.perficient.com/insights/research-hub/mobile-vs-desktop-usage

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., & Gill, P. (2018). Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem. February. https://doi.org/10.14722/ndss.2018.23353

Smyrnaios, N. (2018). *Internet oligopoly: The corporate takeover of our digital world*. Emerald Group Publishing.

Statista. (2021). Number of mobile app downloads worldwide from 2016 to 2020. *Mobile Internet & Apps*. Retrieved from https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

Statista. (2021). Number of smartphone users worldwide from 2016 to 2023. *Telecommunications.* Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2015). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, *22*(e1), e28-e33.

Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus.

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

Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O'Hara, K. (2013, May). Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?. In *Proceedings of the 5th Annual ACM Web Science Conference* (pp. 463-472).

Appendix A – Questionnaire (in Croatian)

ONLINE PONAŠANJE MOBILNIH KORISNIKA

Anketa u prilogu dio je istraživanja u sklopu diplomskog rada Dine Hrastović na Fakultetu političkih znanosti u Zagrebu. Cilj istraživanja je ispitati ponašanje mobilnih korisnika u Hrvatskoj. Više o dizajnu istraživanja i temeljenim teorijama možete pročitati na kraju same ankete, a za sva pitanja javite se na dina@hrastovic.com.

Sudjelovanje u anketi je anonimno. Klikom na SUBMIT na kraju ankete dajete privolu da se podaci koje podijelite tijekom ispunjavanja ankete koriste u svrhu navedenog istraživačkog rada.

Koliko vam je godina? [_____]

S kojim se rodom identificirate? [žena / muškarac / nebirnarna osoba]

Najviši stupanj obrazovanja koji ste završili? [nemam završenu osnovnu školu / osnovna škola / srednja škola / preddidplomski ili diplomski studij / specijalistički ili doktorski studij]

U Koliko veliko naselju živite? [selo ili manje mjesto (do 2000 stanovnika) / mjesto ili grad (do 10 000 stanovnika) / grad od 10 000 do 100 000 stanovnika) / grad s više od 100 000 stanovnika]

U sljedećem koraku vas molim da uskladite odgovor s podacima s vašeg mobitela.

Za korisnike Android mobitela: u Postavkama potražite 'Digital Wellbeing'

Za korisnike Apple mobitela: u Postavkama potražite 'Screentime'

Na novootvorenoj stranici pronađite podatke za prošlu srijedu - koliko ste vremena ukupno proveli koristeći mobitel i koliko ste vremena proveli na top 5 aplikacija tog dana. Ukoliko vam aplikacija ne nudi statistiku za pojedinačni dan, odaberite prosjek za prošli tjedan.

Pronašla sam sve podatke. [DA / NE]

Upišite točno podatke s mobitela. Ako podatke niste pronašli u postavkama mobitela, molim vas da ih pokušate procijeniti na temelju vašeg jednog prosječnog dana.

Ukupno vrijeme provedeno na mobitelu: (u satima i minutama) [_____]

Top 1 aplikacija: [_____]

Top 2 aplikacija: [_____]

Top 3 aplikacija: [_____]

Top 4 aplikacija: [_____]

Top 5 aplikacija: [_____]

Top 5 aplikacija koje ste upravo upisali imajte na umu i nastavite s upitnikom.

Razmislite o tim aplikacijama. Jesi li zabrinut(a) ... [Likert skala (5) / jako sam zabrinut(a) – uopće nisam zabrinut(a)]

- za svoju privatnost generalno dok koristiš te aplikacije?
- zbog online organizacija koje tvrde da su nešto što nisu?
- da te se traži previše osobnih podataka kada se registriraš i nastaviš koristiti aplikaciju?
- da će ti netko ukrasti online identitet?

- da ljudi online nisu oni koji tvrde da jesu?
- da bi informacije o tebi mogle biti pronađene na starom mobitelu?
- da ljudi koje ne poznaješ koriste osobne informacije o tebi iz tvojih online aktivnosti?
- da poruku koju pošalješ online može pročitati netko drugi osim osobe kojoj si poslala/poslao tu poruku?
- da poruku koji si poslala/poslao nekome online može biti neprikladno proslijeđena drugima?
- da poruke koje primaš online nisu od ljudi kakvima se predstavljaju?

Koliko su sljedeće tvrdnje istinite za tebe? [Likert skala (5) / uopće ne znam – sasvim znam]

- Znam kako deaktivirati svoj korisnički račun.
- Znam kako ograničiti pristup podacima mojih korisničkih računa poput povezanih korisničkih računa, interesa i slično.
- Znam kako učiniti svoj račun nedostupnim putem Google tražilice.
- Znam kako kontrolirati mogućnost povezivanja mog korisničkog računa s drugima poput uključivanja u grupe ili tagiranja na fotografijama.
- Znam kako ograničiti pristup sadržaju koji postavljam online.
- Znam kako ograničiti pristup mojim kontakt informacijama.

Prisjeti se ponovo svojih 5 aplikacija koje si najviše koristila/o prošle srijede. Koliko su sljedeće tvrdnje istinite za tebe? [Likert skala (5) / nikako – svakako]

- Pročitala/o sam njihove Izjave o privatnosti.
- Te Izjave o privatnosti su jednostavne za razumjeti.
- Te Izjave o privatnosti su jednostavne za korištenje.
- Razumijem sve postavke privatnosti na njima.
- Svjestna/an sam svih odgovarajućih radnji koje mogu poduzeti kako bih si osigurao/la privatnost na tim aplikacijama.
- Svjestna/an sam svojih prava privatnosti i odgovornosti dok koristim te aplikacije.
- Otkako sam ih počela/o koristiti, promijenila/promijenio sam postavke privatnosti više puta.
- Uvijek razmislim prije nego što nešto podijelim na tim aplikacijama.

Dijeljenje informacija na tim aplikacijama je … [Likert skala (5) / nikako – u potpunosti]

- Korisno
- Ima prednosti
- Zabrinjavajuće
- Opasno
- Nemarno
- Dobro

Ograničavanje pristupa mojim informacija na tim aplikacijama je … [Likert skala (5) / nikako – u potpunosti]

- Korisno
- Ima prednosti
- Zabrinjavajuće
- Opasno
- Nemarno
- Dobro

Razmislite ponovo o svojim najkorištenijim aplikacijama i odgovorite koliko se slažete sa sljedećim tvrdnjama: [Likert skala (5) / nikako se ne slažem – svakako se slažem]

- Tvrtke koje stoje iza tih aplikacija nisu od povjerenja.

- Tim tvrtkama ne treba vjerovati.
- Te tvrtke nisu iskrene.
- Te tvrtke ne uzimaju u obzir moje interese.
- Na kraju dana, te tvrtke samo žele zaraditi na našim podacima.
- Te tvrtke čine s našim podacima što god žele.
- Pretpostavljam da ih zanima samo njihova korist a ne moja.

Odgovorite koliko se slažete sa sljedećim tvrdnjama: [Likert skala (5) / nikako se ne slažem – svakako se slažem]

- Teško je pratiti sve što se događa online.
- Nesiguran/nesigurna sam što se sve dogodi s mojim osobnim podacima online.
- Nesiguran/nesigurna sam što te aplikacije čine s mojim osobnim podacima.
- Nisam siguran/sigurna činim li sve kako bih trebala/trebao dok ih koristim.
- Teško je razumjeti sve rizike kad smo online.
- Ne znam što drugi online korisnici čine s mojim podacima.

Odgovorite koliko se slažete sa sljedećim tvrdnjama: [Likert skala (5) / nikako se ne slažem – svakako se slažem]

- Čak i ako pokušam zaštiti svoje podate, ne mogu spriječiti druge da im pristupe.
- Na kraju, ne mogu spriječiti druge da pristupe mojim podacima.
- Nemam sposobnost učinkoviti zaštititi svoje podate od svih opasnosti online.
- Bilo bi naivno misliti da mogu pouzdano zaštiti svoje osobne podatke online.
- Ako je netko odlučan pristupiti mojim osobnim podacima, ja ništa ne mogu učiniti da ih spriječim.

Razmislite ponovo o svojim najkorištenijim aplikacijama i odgovorite koliko se slažete sa sljedećim tvrdnjama: [Likert skala (5) / nikako se ne slažem – svakako se slažem]

- Nema smisla trošiti toliko pažnje na zaštitu osobnih podataka online.
- Ne mogu trošiti toliko vremena na zaštitu podataka online.
- Odustala/odustao sam od pokušaja da pratim najnovija rješenja kako bih zaštitila/zaštitio svoje osobne podatke online.
- Bezbrižna/bezbrižan sam sa svojim osobnim podacima jer je nemoguće efikasno ih zaštititi.
- Pokušam li zaštiti svoje osobne podatke online ili ne, ne čini nikakvu razliku na kraju dana.

Dijeljenjem osobnih podataka s ovim aplikacijama, koliki benefit dobivate? [skala 0 – 10]

Dijeljenjem osobnih podataka s ovim aplikacijama, koliko riskirate? [skala 0 – 10]

Abstract

Despite the growing awareness of business practices and data harvesting done by leading digital companies in the world, online users seem not to behave in such a way as to protect their data from the ongoing exploitation. This phenomenon has been named the privacy paradox. Recent meta-analysis (Kolokakis, 2019) has shown how inconclusive the consideration and research of the privacy paradox have been. Privacy cynicism is a novel approach to discussing the paradox and is proposed as consisting of four distinct parameters that were developed from the existing literature on cynicism – mistrust, uncertainty, resignation, and powerlessness. The aim of this study was to test this phenomenon among Croatian mobile app users, as there has already been proven the presence of the privacy paradox by an earlier study (Pavuna, 2019). The results indicate there is little to any relations between the often-used predictors of online privacy behavior and the behavior as such. For example, neither have privacy literacy, privacy concerns, nor privacy attitudes influenced privacy protection behavior. The only predictor of the examined behavior was one of the four privacy cynicism parameters – resignation. Whereas other cynicism parameters had a relationship with other assumed predictors of privacy behavior that were not confirmed by this study, resignation remained independent of the rest of the model. Most findings about privacy cynicism in the model supported the findings of Lutz et al. (2019).

Key words: personal privacy online, critical theory of digital media, privacy paradox, privacy cynicism