JOURNAL OF DIGITAL SOCIAL RESEARCH

WWW.JDSR.IO ISSN: 2003-1998

VOL. 3, NO. 1, 2021, 119–152

PRIVACY ATTITUDES AND BEHAVIORS IN THE AGE OF POST-PRIVACY: AN EMPIRICAL APPROACH

Nicolas Demertzis* **, Katerina Mandenaki* ** and Charalambos Tsekeris**

ABSTRACT

The digital world is a field of information and entertainment for users and a field of extraction of the most valuable good of recent years: personal data. How much of a threat to privacy is the collection and processing of data by third parties and what do people think about it? On the occasion of the extensive methods of surveilling citizens and collecting their data, this study attempts to contribute new empirical data evidence from the international research on the use of the Internet by the World Internet Project on attitudes and behaviors of individuals regarding online privacy and surveillance. The aim is to determine whether and to what extent the recorded concerns about the violation of privacy intersects with a growing acceptance of its very absence.

Keywords: World Internet Project; privacy; surveillance; social media; social capital

* National and Kapodistrian University of Athens, National Centre for Social Research (EKKE).
** National Centre for Social Research (EKKE) - Research Associate, Greece.

1 INTRODUCTION

From a free and decentralized research and communication tool, the internet has been transformed in recent years into a commodified space without which we can hardly imagine our lives. Various entities operate with a totally new business model, while major players such as Google, Amazon, Facebook, Apple, and Microsoft (GAFAM) offer innovative and mostly 'free' information, communication, sharing and access services, provided conveniently and quickly from the comfort of our home or wherever we are (de Bustos & Izquierdo-Castillo 2019). With a small exchange: they know who we are, when is our birthday, what are we searching for online, our employment, where we have been, what our faces - and those of friends and relatives - look like, what we believe in, even our political views (Curran, 2018; Smith, 2020; Nield, 2019; Norval & Prasopoulou 2017).

This study seeks to contribute with new empirical data to the investigation of citizens' attitudes, concerns and perceptions on issues of online privacy deriving from the World Internet Project in Greece (WIP-GR), implemented by the National Centre for Social Research (EKKE) [1] as part of the internationally collaborative World Internet Project (WIP).[2] The data related to concerns about privacy and online protection highlights a paradox, as these concerns are counterbalanced by the growing engagement of individuals in online experiences and their acceptance that there is no longer any privacy online: users tend to believe that having '*nothing to hide*' makes it acceptable to concede their data to companies or governments oblivious to the fate of those data.

According to the report by Tsekeris (et al. 2019) Greece is one of the allegedly weakest links of the EU Digital Single Market (DSM)[3] although the EU Digital Economy and Society Index (DESI) for 2020 indicates that the country made the most progress compared to the previous year (especially in connectivity and human capital)[4]. However, it is rather obvious that the so-called 'post-crisis Greece' has a long distance to cover compared to other countries. For 2020, the country, in overall, ranked again 27th out of the 28 EU Member States and still belongs to the low-performing group of countries along with Romania, Bulgaria, Italy, Poland, Hungary, Cyprus, and Slovakia. So, although Greece marginally improved its performance regarding its human capital and the supply side of digital public services, it is placed for one more year under the EU average. Nevertheless, Greeks are still considered to be active users of internet services with their number growing (OECD 2019). In addition, the progress in integrating digital technology has been slow. According to the 'eGovernment Benchmark 2019' [5], Greece is at 27% regarding the penetration of e-services, while the EU average is 57%. In the field

[1] https://www.ekke.gr/
[2] http://www.worldinternetproject.com/
[3] https://ec.europa.eu/digital-single-market/
[4] See full scoreboards here: https://ec.europa.eu/digital-single-market/en/scoreboard/greece
[5] https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2019-trustgovernment-increasingly-important-people

of digitization of public services, the country stands at 51%, far below the European average (68%). However, it seems that Greece has been provided with a significant boost from an unlikely quarter, that is, the coronavirus. The COVID-19 pandemic, the world's first digital pandemic and the ensuing lockdown acted as a catalyst as the country has indeed prompted a rush to adopt massive digital solutions for everything from Cabinet meetings to prescriptions (Stamouli, 2020).

But as in other countries, in Greece the pandemic has once again stirred up the debate on privacy issues. Numerous Greek scholars argue about the biopolitics of the pandemic and emerging anti-democratic tendencies (Douzinas, 2020; Kontiades 2020; Spourdalakis 2020) and collective-cultural drama (Demertzis 2020; Demertzis and Eyerman 2020). Others highlight the way governments, like in Hungary, pushed for authoritarian policies with accelerated procedures (Tzarelas, 2020: 315). In cases such as in Australia, China, Italy, Mexico, Singapore, South Korea, and the US, governments in collaboration with private companies, implemented even more generalized and indiscriminate methods of monitoring citizens and collecting data to observe the spread of the virus without them knowing (Tzogopoulos, 2020; Stein 2020; Singer & Sang Hun, 2020). Furthermore, elsewhere, e.g., in Israel, the government allowed the Secret Services to carry out mass surveillance in mobile phones without a court order to control the increase curve of COVID-19 cases (Gross, 2020). However, the sensitive data collected during this crisis were not only exchanged between health organizations and public health services, as Stein (2020) reveals, since in the US the public services activated applications and digital tools as well as location data from Google and Facebook providing these companies with access to confidential information of citizens such as the date they may have contracted the virus, along with their nationality, gender, age and location. Helbing (2020) notes the crisis seems to have pushed states not only towards obligatory testing, but also towards mass surveillance of data on health, on movement, on contacts, towards mass storage of such data, and potentially, later, towards immunity certificates. Apparently, millions of people are experiencing a bio-political condition that can potentially create new modalities of subjection and subjectivation[6]. It has to be noted, however that on various cases, democracies, especially in Western Europe, decided to preserve their citizens' privacy and informational self-determination [7].

In general, the digital life -in Greece and everywhere else- enmeshes with the multiple structural transformations associated with the rise and spread of the so called 'information and communicative capitalism' (Fuchs, 2012) or 'surveillance capitalism' (Zuboff, 2019). It is also related to the experience of late-modern subjects and societies, thus posing the urgent need for a far greater conscious-raising

[6] https://identitiesjournal.edu.mk/index.php/IJPGC/announcement/view/44

[7] In Germany for instance, as the latest debates and decisions on tracking applications for smartphones show, a new framework for the digital society is on its way – one based on decentralization, the right to maintain one's private sphere, and freedom to choose (Busvine & Rinke, 2020)

and awareness to the situated, cultural and sociopolitical contexts of its use (Fuchs, 2015). It is in the same spirit of critical inquiry that the collective and interdisciplinary World Internet Project (WIP) focuses on the specific national settings of internet use, with analytic attention on comparative and international perspectives. Hence, WIP examines the internet as something more than a global information machine or a communication medium. It emphasizes the cultural and sociopolitical dynamics of the constituent internet technologies, as well as the vast complexity of new types and processes of meaningful action, interaction, experience, subjectivity and identity formation that stretch across the turbulent digital world, especially after the triumphal advent of Web 2.0 or Social Web (Tsekeris & Katerelos, 2014). Emanating from WIP-GR, this paper, first, seeks to overview dataveillance and the datafication of society; second, it refers to the privacy paradox and the resignation of individuals to controversial practices of privacy violation despite them being aware of these violations; third, it attempts an explanatory approach to this contradiction through the exploration of social capital and the emotionality of the public sphere; fourth, it presents our analysis of the WIP-GR 2019 data related to privacy and surveillance and attempts to investigate three questions:

1. Does the level of internet engagement affect people's attitudes concerning their online privacy?

2. Do sociodemographic features predict people's attitudes towards online privacy?

3. Which variable predicts the 'I have nothing to hide' attitude?

Our results show that Greek people are on the track of a rather abrupt transition from digital users to digital citizens. The majority of the participants express their concerns about their privacy being violated as they actively try to protect it. However, more than half of the respondents state that they 'have nothing to hide'. We opted to investigate this conviction and we discovered that Greek people have a rather obfuscated idea about the very notion of digital privacy which might undermine their digital citizenship: they tend to identify it with being 'innocent' of controversial activities therefore being transparent and opening themselves up for datafication but still require protection from their government and expect it to exercise further regulation.

2 THIS DATAFICATION AND POST-PRIVACY IN THE ECONOMY OF CONNECTIVITY

Long before the outbreak of the global health crisis, the advent of social media has allowed companies to target specific groups of users and exploit not only their own data but also the data they generate (metadata) when sharing content or communicating with others (Fuchs, 2014). This 'dataveillance' allows governments and corporations to observe and surveil individuals for the purpose of an

unprecedented concentration of personal information and a form of control (Clarke, 1994), as the Snowden files revealed[8] (Lyon, 2014) or as the interviews with the former director of the US National Intelligence Service, Michael Hayden, describe (Hayden, 2014)[9]. This arguably confirms Christian Fuchs (2014: 92) that 'the actual practices of data marketing, control of media as well as corporate and state oversight restrict the liberal freedom of thought, opinion, assembly and association'.[10]

In the universe of GAFAM, a 'non-alternative' is introduced: providing the software and hardware foundations of the entire internet it is almost impossible for users not to engage with their products and services and not to give in to the cost of their 'free' offering: their data. In the '*platform capitalism*' (Srnicek, 2017) the new economy operates through connectivity as the main resource that marks a systemic shift in the process of profitability. As Mark Zuckerberg testified in 2018 to the U.S. Senate Examination Committee, the business model of Facebook and Google is to provide free services to users in exchange for their data. (Hsu & Kang, 2018; Watson, 2018).

Data monitoring and harvesting has been studied for decades (Rule et al. 1983; Clarke, 1994; Derikx et al. 2015). According to Lyon (2001a), the systematic attention given to people's lives is part of a broader process of maintaining social control and economic management, but in order to achieve this control, the boundaries between the private and the public must be blurred. Information technologies play a central role in this, minimizing the cost of obtaining personal information - without obvious social costs - and increasing 'information asymmetry' (Laudon, 1997; Acquisti et al. 2016). Therefore, the information mosaic of the digital selves is the basis of a relationship that goes beyond digitization and leads to datafication (van Dijck, 2014; Mai, 2016). If digitization allowed for greater storage and faster processing of information, datafication allows it to be transformed into shapes that can be quantified, classified, and analyzed in more sophisticated ways (Mayer-Schonberger & Cukier, 2013) in gigantic aggregations raising numerous issues[11]. As van Dijck (2014) notes, even academia has embraced the datafication paradigm by 'assessing big data sets collected through social media platforms as the most scrupulous and comprehensive method to measure quotidian interaction, superior to sampling ('N=all') and more reliable than interviewing or polling' and 'assuming a self-evident relationship between data and people'. What is missing though is that the allegedly 'objective' nature of quantitative analysis cannot exist without a qualitative, critical framing that guides the research with a quite subjective, intentional manner.

[8] https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi

[9] Hayden also commented that following September 11 the CIA "could be fairly charged with the militarization of the world wide web." (Peterson, 2013)

[10] cf. Fuchs, 2015· Cammaerts, 2008· Hindman, 2009· Mosco, 2009.

[11] Cf. ethics of information (Lyon, 2001b), legal issues (Schuster et al. 2017), identification of personal data (Fuchs 2012) exploitation of information for profit (Van Dijck, 2013)

It seems like there are two major starting points for this unprecedented information aggregation and control. First, it was the USA legislative statute known as Section 230 of the Communications Decency Act[12], which was crafted in 1996, during the initial phase of the public internet. It states that '*no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*'. The aim of the statute was to clarify intermediaries' liability for the content on their websites, but it inevitably shielded website owners from lawsuits and state prosecution for user-generated content. Thank to this regulatory framework sites like Booking.com can defend even aggressive negative hotel reviews and Twitter and Facebook allow trolls and fake news to 'roam free' without either company being held accountable to the same standards that news organizations are. As it institutionalized the idea that websites are not publishers but rather 'intermediaries', this statute not only freed them from the responsibility of their content (or its providers), but it ended up sheltering the extractive operations of this very content from critical examination. The second milestone came six years later, in the aftermath of the September 11th attacks in USA, when the government's concerns shifted from online privacy protections to a new need for 'total information awareness' (Rosen, 2002) as an unwritten policy of 'surveillance exceptionalism' (Zuboff, 2019) emerged. Legislation to regulate online privacy became a casualty of the 'war on terror', the 'goods' produced in Silicon Valley evaded legislative action and became highly coveted as was the need for higher speed in clandestine digital services.

Harvesting data is not a novel phenomenon (Flick, 2016). What is new is the extent of exposure of this data and how it can be aggregated and transformed uncontrollably (Van Dijck, 2014; Mai 2016). In 2019, the French Commission for the Protection of Personal Data (CNIL) fined Google €50 million for violating EU privacy rules, 'for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization'[13]. Earlier, on the other side of the Atlantic, an investigation by the *Observer* and the *New York Times* revealed that 50 million Facebook user profiles were processed by Cambridge Analytica, creating a program that could predict and influence their electoral behavior sending them targeted and personalized messages based on their data[14]. Moreover, the same investigation revealed that in addition to the US election, the same method was used to manipulate the results of the 2016 British referendum that led Great Britain

[12] Section 230 of the Communications Decency Act, Electronic Frontier Foundation, https://www.eff.org/issues/cda230.

[13] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc; See also https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog

[14] According to information provided by Christopher Wylie the whistleblower that uncovered the story: "we exploited Facebook to collect millions of user profiles and create models to tap into what we knew about them and target their inner demons." Cf. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

to the infamous Brexit pivoting for the first time the whole dataveillance undertaking from commercial to political objectives.

This kind of targeted advertising invented by Google (Zuboff, 2019: 67) paved the way to economic success but also laid the foundation of a 'surveillance capitalism' with 'idiosyncratic economic imperatives defined by extraction and prediction, a 'unique approach to economies of scale and scope in raw-material supply'. Surveillance capitalism begins by unilaterally making a claim to private human experience as free 'raw material' for transformation into behavioral data, making data the very element tech giants may assert authority over -the same way oil companies assert authority over crude- in order to achieve economies of scale in its raw material supply operations. And in transforming 'crude' data into information 'gasoline', GAFAM's machine intelligence operations convert human experience into the firm's highly profitable algorithmic products designed to predict the behavior of its users (Zuboff, 2019).

Profits in the 'attention economy' (Davenport & Beck, 2013; Boyd & Crawford, 2012) comes from the customization and personalization of the information extracted, thus influencing people's attention, emotions, and behaviors (Demertzis & Tsekeris, 2018). The combination with other communication techniques such as neuromarketing (Zurawicki, 2010; Ariely & Berns, 2010), neurobranding (Steidl 2012) or automated social media bots (Shorey & Howard 2016), may generate very effective propaganda, manipulate or even deceive. The ongoing debate about fake news and post-truth society (Keyes, 2004; McIntyre, 2018) as well as post-democracy (Crouch, 2004) can be conducted under a new light in this 'post-privacy' era (Heller, 2011).

Moreover, as today's advertisement is capitalizing on digital technologies to dig further into the needs, interests, and motivations of customers, behavioral advertising, online profiling and 'behavioral targeting' while being shielded from any accountability as to the nature of the content targeted, have become common tactics for suppliers to effectively sell products to customers in the digital environment. Especially in cases of electoral choice, adding to personal profiling based on user activity and interests, 'affinity profiling' (Wachter, 2020) classifies people based on their assumed interests according to groups they supposedly belong to, thus providing online platforms with sensitive information such as ethnicity, gender, sexual orientation or religious beliefs. What is called 'affinity profiling', or profiling which seemingly does not directly infer sensitive data but rather measures an 'affinity' with a group defined by such data (Wachter, 2020), not only violates privacy but might even unlawfully discriminate against users who receive inadequate legal protection as groups. A violation which could undermine the application of the EU General Data Protection Regulation (GDPR) against processing of sensitive data.

3 THE 'PRIVACY PARADOX' AND THE NON-PRIVATE NATURE OF PRIVACY

These practices do not seem to prevent people from using the internet, accepting cookies when visiting a website or participating in social media (Ngwenyama & Klein 2018, Van Dijck 2013). Norberg et al. (2007) coined the term 'privacy paradox' to describe the dichotomy between individuals' willingness to concede their data with almost negligible rewards and their expressed concerns about the violation of their privacy (Kokolakis, 2017). The bloodless 'coup' that has been inflicted on modern societies by digital moguls relies, 'on the most treacherous hallucination people have: that 'privacy is private' (Zuboff, 2021). And giving away or conceding a bit of personal information is a fair 'quid pro quo' if users can get extra service. For example, when Delta Air Lines piloted a biometric data system at the Atlanta airport, the company reported that of nearly 25,000 customers who traveled there each week, 98 percent opted into the process, noting that 'the facial recognition option is saving an average of two seconds for each customer at boarding, or nine minutes when boarding a wide body aircraft.' (Zuboff, 2020; Murgia, 2019). Privacy is not private, because the effectiveness of all private or public surveillance and control systems depends upon the pieces of ourselves that we give up -or that are secretly taken from- even through seemingly innocent micro-activities such as clicking on an angry emoji under a disliked post on Facebook: opinions are collected, assessed and treated as property. And that transaction takes place in a totally asymmetrical distribution of knowledge, as tech giants have control of information and learning whereas a significant number of people have trouble figuring out how to pay their bills online. Unequal knowledge about people produces unequal power over them. And from algorithms that profile people to predict their behavior, surveillance capitalism is reaching a point where predictive knowledge is morphing into modification power as was shown in Facebook's contagion experiments (Bond et al., 2012; Kramer at al., 2014), when it succeeded in modifying human behavior by planting subliminal cues and manipulating social comparisons on its pages, to influence users to vote in midterm elections and to make them feel sadder or happier.

So where does all this leave users' privacy? In an experimental study, Carrascal (et al. 2013) found that internet users priced their internet search history information at around 7 euros, while Egelman (et al. 2012) showed that consumers were willing to pay a price to buy the protection of their privacy but it was a small one.[15] Earlier research on user attitudes indicated that privacy and the collection of information is something that particularly concerns users (TRUSTe 2014; Madden 2014) although they can give it away as soon as they realize there is something to gain (Brown, 2001; Spiekermann et al. 2001). Taddicken (2014) showed that privacy concerns do not affect self-disclosure if the communication pattern between users is performed on an exchange basis like '*tell me about you and I will tell you about*

[15] Users were not willing to pay more than $ 1.50 to 'buy' the security of their privacy.

me' or includes the benefit of shareability (Lee et al. 2013). Zafeiropoulou (et al. 2013) investigated users' attitudes about their location data and discovered that even in this case that concerns a particularly sensitive information,[16] users willingly reveal it or provide constant access to it in exchange for participating in an internet activity or enjoy a free service. Ngwenyama & Klein (2018) argue that the compliance of individuals with controversial practices of privacy violation is due to a voluntary 'amnesia' and a lack of awareness related to the confusing nature of social media surveillance practices. They concluded that data monitoring, control and financial exploitation involve ethical contradictions, covert purposes, agendas and ideology.

Examples like that lead to what Draper & Turow (2017) call 'digital resignation', arguing that the very notion of the '*privacy paradox*' is faultily burdening users: people do not give up personal information just to get discounts or services nor do they lack comprehension for the consequences of that disclosure. They do so because they are accepting as inevitable the undesirable ways marketers use personal information and resign to them. A purposeful strategy of commercial interests and not an accidental byproduct of 21st century digital life, 'digital resignation' is something to investigate on multiple institutional and societal levels and understand its nature and origins. Internet users cannot learn enough about privacy risks to make informed decisions about their privacy as it is impossible to gain sufficient knowledge of the ways in which personal data are processed and analyzed by thousands of organizations and numerous obscure techniques. The advent of large-scale 'Big Nudging' (Helbing, 2015) and 'Big Data surveillance' (Lyon, 2014), has established omnipotent technologies of control, calculability and prediction (Kucklick, 2014), which, produces unprecedented power asymmetries between the state and its citizens, (Brunton & Nissenbaum, 2015) and corporations and their customers. According to the JRC Science for Policy Report of the European Commission (2020)[17], companies use several questionable techniques like *defaults*, *framing*, *nudging* and *dark patterns* to build choice architectures and dissuade users from making active or informed choices leading not only to the sharing of personal information but to manipulation and deception. For instance, framing and wording may be used to nudge users towards a choice by presenting the alternative as risky (e.g., on Facebook, users are encouraged to keep face recognition turned, because it ostensibly helps 'protect you and others from impersonation and identity misuse and improve platform reliability.')[18]. Choice architectures may also require a take-it-or-leave-it decision, like a choice between accepting specific privacy terms or deleting an account. They may even be designed

[16] Although geolocation data are not considered "sensitive" in a legal point of view they are personal and of importance to the safety of users providing very intimate and accurate overview of their habits and patterns. Retaining location data forever and obtaining a single privacy consent for multiple purposes are practices already unacceptable. https://iapp.org/news/a/what-the-gdpr-will-mean-for-companies-tracking-location

[17] https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/technology-and-democracy

[18] https://www.facebook.com/help/122175507864081

in such a way that the privacy-friendly option requires more effort and knowledge from users. The very task of trying a 'self-managed privacy' is futile so long as the various decisions people must make about their privacy and the tasks they must do regarding it (reading privacy policies, opting out, changing privacy settings etc.) make it a complex and never-ending project (Solove, 2013; 2020). Resignation is a rational response to the impossibility of privacy self-management rather than a voluntary servitude.

4 SOCIAL CAPITAL IN THE EMOTIONAL PUBLIC SPHERE

There is a number of further aspects influencing users' interest in protecting their privacy on the Internet, their attitude towards others and the very ability to be anonymous online. Active participation in social networks associated with self-disclosure is related to three needs: the need for entertainment, for social relationships and the need to construct identity (Debatin et al. 2009). For most users, meeting the above needs outweighs the risks of personal data exposure and privacy violation by responding to a 'ritualistic' integration of online socialization. Social networking is a way of gaining social capital (Ellison et al. 2011) that is exchanged for the disclosure of personal information[19]. Demertzis & Tsekeris (2018: 16) note that the tools and control mechanisms involved in the 'governmentality of the neoliberal debt economy' create new emotional rules, informalize behaviors and compose an emotional public sphere in which people, freed from the constraints of the past, express themselves freely following the track of the '*emancipation of emotions*' (Wouters, 2007). If the concession of private information is the cost of engaging networked but disconnected individuals in the 'emotional public sphere' where narcissistic disclosure of emotionality takes place in the name of '*authenticity of the self*' (Sennett 1993), then the benefit may be considered great.

It seems, however, that people are beginning to doubt the data-for-free-services-exchange they have involved themselves too. According to Pew Research Center[20], 81% of Americans believe the potential risks of companies' data collection outweigh the benefits but they have no comparable alternatives of living their digital lives (Auxier et al. 2019). So, where do Greek people place themselves in this landscape of distorted digital communication?

[19] Stutzman et al (2012) have shown that if a person reveals a medical problem, they are more likely to attract sympathy and support from members of their network.

[20]https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

5 WIP-GR SURVEY: SAMPLE DESCRIPTION AND DATA DEFINITIONS

The third wave of WIP-GR[21] was implemented in Spring 2019 by the National Centre for Social Research (EKKE)[22] as part of the international World Internet Project (WIP). WIP is a major survey-based research program, launched in 1999 and directed by the Annenberg School Center for the Digital Future at the University of Southern California, looking at the social, political and economic impact of the internet, as well as at how individuals adopt and use the internet and other new technologies, and what implications this has on their everyday lives and communities. This program becomes increasingly important because in order to get closer to the kind of internet we want, 'we need a better understanding of the internet that we have' (Bernal, 2018: 2).

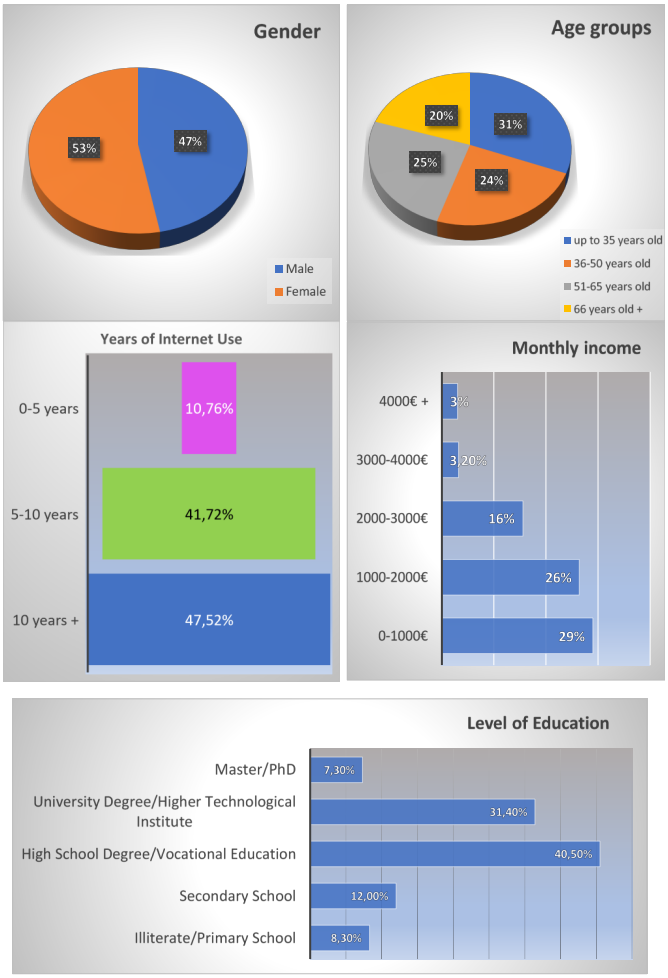

Figure 1: Demographic features

[21] The first wave of the survey in Greece was conducted in November and December 2015, and the second between 31st January and 21st February 2017. The present study offers a comprehensive presentation of the empirical results of the third wave of the survey, which was conducted between 12th April and 23rd May 2019.
[22] https://www.ekke.gr/

The research methodology was designed by EKKE and 1,208 interviews were conducted by using a structured questionnaire via CATI by trained interviewers from EKKE's Web Lab. The data were collected 12 April – 23 May 2019 and cleaned accordingly. [23] There are several modules in the questionnaire explored for the purpose of this study. The demographic variables we utilized are: Gender, Age, Education, Internet use experience and Monthly income (See Figure 1).

In the total sample both genders (women 52% - men 47%) were almost equally represented while the age span of the participants was from 15 to 97 years. Almost half the respondents are early Internet users with 10+ years of experience. The majority of the participants have either High School diploma or vocational training and one third possess a University degree. Finally, half our respondents are economically located in the lower to middle income levels with a minority of 6% stating a higher financial status.

6 RESEARCH QUESTIONS AND METHODOLOGY

To clarify privacy attitudes among Greek users, we followed a two staged strategy. First, we investigated what Greek uses are more concerned about presenting metrics on 5 statements measuring privacy attitudes and 4 statements [24] measuring respondents' perceived safety for exercising their freedom of speech online. On the second part of our research, we analyzed our data. First, we created scales to measure internet engagement and social media use in order to investigate the degree to which online convenience and gaining social capital affect peoples' attitudes. Second, we correlated the scales and the sociodemographic characteristics of our users with their attitudes. Finally, we opted for an interpretation of the '*I have nothing to hide*' attitude to determine whether it is an indication of digital resignation that justifies a more submissive attitude on behalf of our participants. The above are tested in the following research questions:

Q1: Does the level of internet engagement affect people's attitudes concerning their online privacy?

Q2: Do demographic features predict people's attitudes towards online privacy?

Q3: Which variables predict the attitude 'I have nothing to hide'?

[23] The dataset was weighted according to the 2011 Population Census and the Labor Force Survey.
[24] The statements were measured on a 5 grade Likert scale from "strongly agree" to "strongly disagree".

7 FINDINGS: PRIVACY ATTITUDES AND CONCERNS

7.1 Privacy concerns-descriptive statistics

As can be seen in Figure 2, 54% of the respondents claim that '*There is no privacy, accept it*', whereas only 23% somewhat and strongly agree with the statement that '*concerns about online privacy are exaggerated*'. Almost 60% of the users feel they '*can control*' their privacy online, and 70% state that they '*actively protect*' it. Furthermore, we observed a dichotomy between the meaning the majority of the respondents' attributes to the statement *I have nothing to hide* (55,8%) and their strong concerns about their privacy being violated by corporations (75.6%), the government (60.8%) and other people (62.2%).

*Figure 2: Privacy Concerns and attitudes**

In the WIP-GR survey the biggest concern about online privacy being violated is about *corporations* which is probably explained by the fact that most users often receive targeted advertisements and several digital marketing products. It is not enough for a company like Facebook to store 300 million photos or record the 2.7 billion likes that are clicked daily; using several algorithms, it mines this data, processes, and combines them committing 'abuse through transformation' (Schyff et al. 2018; Smith (2016).

Another concern for 62% of the respondents is about governments. Governments surveil citizens and collect information and data to deal with cybercrime, fraud, terrorism, or other violations (Amoore & De Goede 2005), to establish a more efficient bureaucracy or to control immigration. As shown in

Figure 3, the WIP-GR research participants express caution and an underlying awareness.

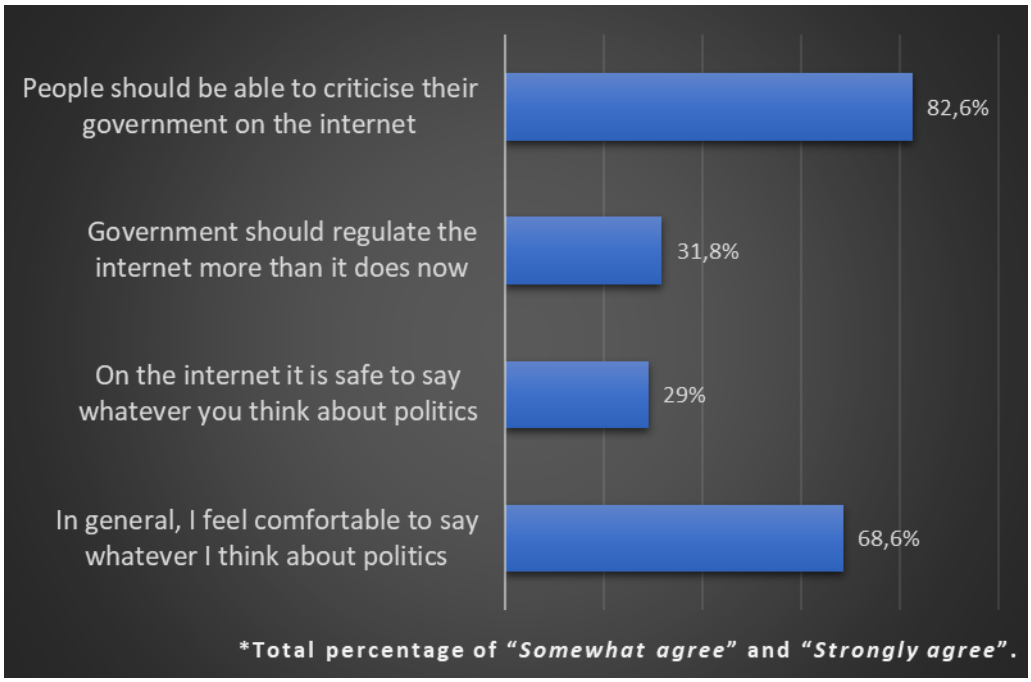

*Figure 3: Freedom of Speech**

The grand majority hold that '*people should be able to criticize their governments online*' (86%). Fewer respondents state that they feel '*comfortable saying whatever they think about politics*' in general (68%) -admittedly denoting a significant degree of freedom of speech in Greece- however, much fewer believe that the internet is a safe place to express political ideas (27,20%). In the same vein, more than four out of ten people (48%) reject potential increase of internet regulation by the government. Apparently, participants believe that the internet ultimately involves the risk of exposing their political profile both to centers of power that may be surveilling them and to opposers who may be attacking. Political cyberbullying is a raising issue in various online communities (Bauman, 2019), while in the American elections of 2016 the phenomenon was seriously escalated especially due to the inflammatory rhetoric of Presidents' Trump campaign.[25]

In addition to companies and governments, personal data are also being coveted by other individuals with controversial goals, mainly of a delinquent nature, such as identity theft, bank robbery, blackmail, or harassment, a danger that concerns 63% of Greek users. Apparently, users' concerns about the violation of their data by other individuals are associated with 'social privacy' which differs from 'institutional privacy' and violations by companies or governments (Park et al. 2018). In short, collecting and processing data from the socio-economic background of users for the purpose of profit or control does not seem to bother them as much as e.g., having to deal with embarrassing photos being posted on

[25] www.sciencedaily.com/releases/2019/01/190109090917.htm

Facebook by a malicious person. This is an indication of a cognitive dichotomy, given that users worry about something they haven't really experienced while high rates of concerns about violations by others indicate that the issue of privacy appears to be a matter of infringement, criminal activity or social exposure and ashaming. It is also likely that respondents have not assessed several mundane cases as indicative of privacy violations, like targeted ads or recommendations to rate restaurants or cafes as soon as they exit them.

8 ANALYSIS

8.1 Q1: Does the level of internet engagement affect people's attitudes concerning their online privacy?

We implemented twenty-two variables and conducted an exploratory factor analysis (Floyd & Widaman, 1995; Gorusch, 1990) to develop scales that would measure peoples' level of internet engagement (deVellis 2003). We used principal axis factoring (Worthington & Whitaker 2006) with Promax (orthogonal) rotation. To estimate the contribution of specific socioeconomic variables to respondents' attitudes, we focused on gender, age, monthly income, and education level and implemented multinomial logistic regression (Gould, 2000; see also Papadoudis 2018). Ordinal regression analysis was used to determine what are the convictions of people who believe they have *nothing to hide.*

The analysis yielded three factors explaining a total of 47,266% of the variance for the entire set of variables (see Table 1). Factor 1 was labeled 'O*nline Sociability*' due to the high loadings by items such as: frequency of posting content, sharing content, instant messaging and phone calls online, maintaining relationships, create relationships, download videos and music. The second factor was labeled '*Internet use Frequency*' due to the high loadings by items concerning how often users go online for several activities e.g., to get information about a product, buy things, make travel reservations, pay bills, etc. The third factor was labeled '*Internet Proficiency*' because the 4 items that loaded onto it were related to the users' self-declared level of knowledge of performing tasks on the internet and their ability to effectively navigate it. The KMO score (0,843) and Bartlett's Test of Sphericity ($p<0,001$) both indicate that the set of variables is well related. We tested the internal consistency of the items by computing the Cronbach's a score for each factor. Finally, we attributed Anderson Rubin scores (Mean = 0, Variance of 1) to create 3 new variables labeled *Online Sociability scale*, *Internet Frequency Use scale* and *Internet Proficiency scale. (Table 1).*

Table 1: Factor Analysis - Internet engagement scales

	Loadings			***Communality***
	Factor 1: Online sociability (*Cronbach's a =0.837*)	Factor 2: Internet Frequency use (*Cronbach's a= 0.787*)	Factor 3: Internet Proficiency (*Cronbach's a =0.901*)	
Instant messaging	0,711		0,565	0,536
Post your own content (videos, photos etc.)	0,689		0,436	0,477
Maintain your relationship with people with a similar social status	0,681			0,464
Re-post or share links or content others have created	0,642		0,406	0,415
Keep your existing relationships with family/friends	0,576			0,342
Make or receive phone calls over the Internet	0,568			0,323
Download or watch videos	0,537			0,300
Find people of a similar social status	0,499			0,261
Download or listen to music	0,493			0,255
Get information about a product		0,673		0,453
Buy things online		0,661		0,443
Compare prices of products/services		0,572		0,332
Make travel reservations/bookings		0,562		0,318
Look for travel information		0,501		0,253
Pay bills online		0,480		0,236
Find or check a fact		0,479		0,242
Look up a definition of a word		0,435		0,221
Look for news (local, national, international)		0,409		0,169
I know how to create content and upload to the internet	0,562		0,920	0,851
I know how to adjust it to what share content online	0,550		0,891	0,799
I know how to download applications on a mobile phone or tablet	0,435		0,749	0,563
I know how to open a file downloaded from the internet	0,413		0,723	0,543
Eigen value	6,350	2,397	1,652	
% of Total Variance	28,862	10,897	7,508	
Total Variance			47,266	

We created these scales to examine if online sociability, frequency of use and internet proficiency affect people's attitudes towards privacy concerns. We hypothesized that people who score high in online sociability and internet frequency use would be more willing to declare their concerns as conscious users but still exhibit a dichotomy since they are the ones to benefit most from internet's free services and activities. So, we performed a one-tail Pearson correlation to see also the direction. According to the results shown in Table 2 there is a significant deviation in people who score higher in the frequent use scale to be more concerned about corporations violating their privacy online. Another notable finding is people who score highly in both online sociability and internet proficiency tend to disagree with the notion '*I have nothing to hide*' indicating that their involvement in the internet's allure has in fact instilled in them the idea that wanting to be private doesn't mean that you hide something. However, respondents who scored highly on the internet proficiency scale is the only group that disagrees with the statement '*there is no privacy accept it*'. This is a good indication that the 'connoisseurs' understand two things: a) there are ways to protect ones' digital privacy and they probably know about them and b) they are not inclined to yield to the easy refuge of admitting that since there is no privacy online there is nothing we can do other than conceding private information to enjoy free services and social capital. Digital 'socialites' also tend to disagree with this statement but not significantly.

Finally, while initial results showed that the majority of the respondents disagree with the statement '*on the Internet, it is safe to say whatever you think about politics*' (48,3%)[26], if we look closer to the respondents who score high in all three scales, they are most likely to agree with this statement. Being 'safe' to express political views online is not only about evading government surveillance, it also concerns being able to post opinions and participate in online discussions without being bullied. So, respondents who are highly engaged with the internet, possibly are not so concerned of being surveilled by the government rather than being able to handle online bulling and the emotionally charged spaces were politics might be discussed. However, all types of users, socialites, frequent users and connoisseurs tend to disagree with the statement that the '*governments should regulate the internet more than they do now*', an indication of sharing the libertarian culture of netizens initiated already at late 1990s.

[26] Total percentage of "Somewhat disagree" and "Strongly disagree".

Table 2: Correlations between internet engagement and privacy attitudes and behaviors

		Online Sociability Scale '*socialites'*	Frequency use scale '*frequent users*'	Proficiency scale '*connoisseurs'*
Privacy violations by Governments	Pearson r	0,021	0,052	-0,029
	Sig.	0,271	0,068	0,203
Privacy violations by Corporations	Pearson r	0,049	,134**	,066*
	Sig.	0,080	*0,000**	*0,030**
Privacy violations by Other people	Pearson r	-0,020	0,007	0,012
	Sig.	0,287	0,423	0,366
I actively protect my privacy online	Pearson r	0,033	0,023	0,040
	Sig.	0,170	0,255	0,128
Concerns about privacy online are exaggerated	Pearson r	-0,027	-0,020	-0,021
	Sig.	0,216	0,282	0,272
I have nothing to hide	Pearson r	-,101**	-0,016	-,086**
	Sig.	*0,002**	0,320	*0,007**
I feel I can control my privacy online	Pearson r	-0,043	-0,056	-0,008
	Sig.	0,107	0,055	0,410
On the Internet, it is safe to say whatever you think about politics	Pearson r	,138**	,094**	,133**
	Sig.	*0,000**	*0,004**	*0,000**
The government should regulate the internet more	Pearson r	-,089**	-0,053	-,115**
	Sig.	*0,006**	0,067*	*0,001**
There is no privacy, accept it	Pearson r	-0,004	0,015	-,058*
	Sig.	0,449	0,329	*0,048*

***. Correlation is significant at the 0.01 level (1-tailed). *. Correlation is significant at the 0.05 level (1-tailed).*

8.2 Q2: The demographics of online privacy concerns

The theme for this analysis is centered on four demographics and the three constructed scales of internet engagement to examine if these parameters can predict the respondents' privacy attitudes and concerns. For the estimations in Table 3 we implemented multinomial logistic regression reporting coefficients and odds ratios (OR). Each OR takes values higher than 0 and lower or higher than 1 which is the focal point (a value of 1 means that there is no contribution of the variable). Values below or above 1 may also interpret the direction of the attitudes according to which group is set as the reference group. In this case the reference category was *Disagree* because we wanted to use it as a baseline. The regression was performed to model the relationship between the predictor variables and participation in the three response groups (Agree, Disagree and Neither/nor Agree/Disagree). The predictive variables were all treated as covariates. The general significance of the model is good as shown both by the p value ($p<0,005$) in most cases and the χ^2 test. Therefore, the variables contribute to explain the essence of the privacy attitudes and representations of the respondents[27]. There are interesting results coming out of our explorations:

[27] It should be noted that due to the realistic nature of our data there were cases of missing values which we are reporting in the footnote of Table 3.

Concerning gender, women tend to declare they 'actively protect their digital privacy' more prominently than men and they also tend to believe that they 'feel they can control their privacy online'. Women also appear to have given in the 'nothing to hide' concept as they tend to agree with this statement more than men although they do not believe that the internet is a safe place to discuss politics as strongly as men.

The factor of age only seems to affect people's perception about 'having nothing to hide' as they grow older therefore showing a mild positive direction to the statement as younger people appear more strongly in the Disagree side of the statement. We could hypothesize that older individuals, when presented with this statement, might perceive it as a challenge to their personal idea of dignity (they have done nothing wrong) rather than a challenge to their privacy.

The economic status of the respondents seems to significantly affect their efforts to 'actively protect their privacy', the odds ratio of being in the 'Agree' group rather than the' Disagree' are multiplicatively increased by 1,342. Also, the higher the income the less likely is the respondent to agree with the statement that governments violate online privacy (B=-0,230). However, their efforts to actively protect their privacy must be considered along with their significant agreement with the statement that 'there is no privacy online accept it' (OR=1,219), a statement that is mostly rejected by respondents who scored highly on the internet proficiency scale, as was also seen previously in the correlations (Table 2).

An interesting result derived from the variable of education as people of lower educational levels state they more actively protect their privacy online (Figure 6) than the more educated users possibly because people with higher education may realize that actively protecting their privacy will not essentially protect them from violations, since they don't feel they can control it as indicated by the negative coefficient (B=-0,227). However, people with higher education tend to disagree with the statement 'concerns about online privacy are exaggerated' (Figure 7) whereas people with lower education tend to populate in higher percentages the 'Agree' and 'Neither/nor' area of the discussion.

People with higher internet proficiency scores significantly agree with the statement that it is safe to discuss politics online (B=0,275, p=0.004) but they reject the idea that governments should regulate the internet more, as indicated by the negative coefficient (B=-0,288, p=0,036) in the Agree category. 'Connoisseurs' don't believe that there is no privacy online (B=-0,426, p<0,01) however people with higher online sociability scores seem to have accepted this idea (B=0,255, p=0,019).

Table 3: Multinomial logistic regression

Parameter Estimates

Privacy violations by Governments[a] [(x2(14)=26.244, p=0.024)]					I have nothing to hide[f] [(x2(14)=31.707, p=0,04)]			
Agree	B	Std. E.	Sig.	Exp(B)	B	Std. E.	Sig.	Exp(B)
Monthly Income	-0,230	0,092	0,013	0,794	0,197	0,101	0,051	1,218
Age	-0,159	0,117	0,175	0,853	0,385	0,131	0,003	1,470
Gender	0,015	0,193	0,937	1,015	0,400	0,202	0,048	1,491
Level of Education	0,163	0,131	0,212	1,177	-0,127	0,136	0,351	0,881
Online sociability	-0,021	0,118	0,857	0,979	0,010	0,123	0,936	1,010
Internet frequency use	0,198	0,190	0,296	1,219	0,111	0,193	0,564	1,118
Internet Proficiency	-0,195	0,140	0,166	0,823	-0,071	0,144	0,621	0,931
Privacy violations by Corporations[b] [x2(14)=21.708, p=0,08]					I feel I can control my privacy online[g] [(x2(14)=16.131, p<0,001)]			
Agree	B	Std. E.	Sig.	Exp(B)	B	Std. E.	Sig.	Exp(B)
Monthly Income	-0,102	0,126	0,417	0,903	0,181	0,103	0,079	1,199
Age	-0,021	0,159	0,895	0,979	0,189	0,131	0,151	1,208
Gender	-0,194	0,258	0,453	0,824	0,422	0,206	0,040	1,525
Level of Education	0,414	0,174	0,017	1,513	-0,227	0,139	0,104	0,797
Online sociability	-0,087	0,155	0,576	0,917	0,014	0,124	0,911	1,014
Internet frequency use	0,116	0,252	0,643	1,124	-0,209	0,193	0,281	0,812
Internet Proficiency	0,203	0,176	0,248	1,226	0,195	0,143	0,173	1,215
Privacy violations by Other people[c] [(x2(14)=9.189, p=0,819)]					On the Internet, it is safe to say whatever you think about politics[h] [(x2(14)=25,698, p=0,029)]			
Agree	B	Std. E.	Sig.	Exp(B)	B	Std. E.	Sig.	Exp(B)
Monthly Income	-0,046	0,103	0,652	0,955	0,129	0,088	0,145	1,138
Age	-0,237	0,128	0,063	0,789	-0,071	0,114	0,534	0,932
Gender	0,176	0,210	0,402	1,193	-0,634	0,184	0,001	0,531
Level of Education	0,105	0,141	0,458	1,111	-0,116	0,123	0,345	0,890
Online sociability	-0,053	0,126	0,676	0,949	0,143	0,112	0,201	1,154
Internet frequency use	-0,134	0,201	0,506	0,875	0,106	0,175	0,546	1,112
Internet Proficiency	0,041	0,146	0,779	1,042	0,275	0,134	0,040	1,317
I actively protect my privacy online[d] [(x2(14)=26.033,p=0.026]					There is no privacy, accept it[i] [(x2(14)=40.593, p<0,001)]			
Agree	B	Std. E.	Sig.	Exp(B)	B	Std. E.	Sig.	Exp(B)
Monthly Income	0,270	0,117	0,021	1,310	0,157	0,089	0,078	1,170
Age	0,175	0,142	0,217	1,191	0,090	0,111	0,417	1,094
Gender	0,452	0,227	0,046	1,571	-0,100	0,179	0,576	0,905
Level of Education	-0,376	0,154	0,015	0,687	0,018	0,123	0,885	1,018

Online sociability	0,096	0,133	0,471	1,100	0,255	0,109	0,019	1,290
Internet frequency use	0,154	0,216	0,477	1,166	0,076	0,174	0,662	1,079
Internet Proficiency	0,242	0,152	0,112	1,274	-0,426	0,130	0,001	0,653

	Concerns about privacy online are exaggerated[e] [(x2(14)=24.258, p=0,043)]				The government should regulate the internet more than it does today[j] [(x2(14)=25.658, p=0,029)]			
Agree	B	Std. E.	Sig.	Exp(B)	B	Std. E.	Sig.	Exp(B)
Monthly Income	0,099	0,098	0,310	1,105	0,057	0,094	0,541	1,059
Age	0,107	0,124	0,387	1,113	-0,045	0,122	0,711	0,956
Gender	-0,144	0,202	0,477	0,866	0,199	0,192	0,299	1,221
Level of Education	-0,356	0,136	0,009	0,700	-0,277	0,129	0,032	0,758
Online sociability	0,081	0,123	0,509	1,084	-0,019	0,117	0,869	0,981
Internet frequency use	0,082	0,192	0,668	1,086	0,187	0,184	0,308	1,206
Internet Proficiency	-0,043	0,142	0,759	0,958	-0,288	0,138	0,036	0,750

** Significance at the 0.05 level. p≤,005.*

a. Missing=558,36. b. Missing=553,53. c. Missing=555,51. d. Missing = 550,74. e. Missing=551,36. f. Missing= 548,46. g. Missing=550,63. h. Missing=553,92. i. Missing=551,38. *J*. Missing=573,69.

8.3 Q3: Which variable affects the attitude '*I have nothing to hide*'?

So far, the '*I have nothing to hide*' attitude was not explained by any variable, therefore, in order to determine which factors are incorporated in this particular attitude we performed an ordinal regression analysis between the attitudes themselves to determine what are the convictions of people who believe they have *nothing to hide*. As shown in Table 4 the model seems good ([$\chi^2(18)=98.760$, $p<.001$] and it provides us with three significant results deriving from the 'Disagree' category:

1) The attitude '*concerns about online privacy are exaggerated*' was a significant predictor of '*I have nothing to hide*' attitude as there is a predicted decrease of 0.064 in the log odds of disagreeing with this statement as opposed to agreeing. This indicates that a person who believes that concerns about privacy online are being exaggerated is more likely to state they have nothing to hide.

2) The statement '*I feel I can control my privacy online*' was also a significant predictor in the model as there is a decrease of 0.098 in the log odds of disagreeing with the statement. This also indicates that people who feel they can control their online privacy are more likely to state *they have nothing to hide*.

3) Finally, the variable 'the government should regulate the internet more' significantly contributed to the model with a strong inverse relationship of -0,733 to the category 'Disagree' indicating that people who have nothing to hide tend to state that the government should exert a stronger presence in regulating the Internet. These results might indicate people's perception of a digital inefficacy that may lead to a digital resignation regarding their privacy which they may perceive as vulnerable.

Table 4: Ordinal regression analysis 'I have nothing to hide'

*Parameter Estimates**

		Estimate	StdError	Wald	Df	Sig.
Privacy violations by Governments	Disagree	-0,368	0,224	2,700	1	0,100
	Neither agree/disagree	-0,216	0,251	0,742	1	0,389
	Agree	0[a]			0	
Privacy violations by Corporations	Disagree	-0,022	0,288	0,006	1	0,939
	Neither agree/disagree	-0,046	0,295	0,024	1	0,876
	Agree	0[a]			0	
Privacy violations by Other People	Disagree	0,242	0,229	1,125	1	0,289
	Neither agree/disagree	-0,046	0,226	0,042	1	0,837
	Agree	0[a]			0	
I actively protect my privacy online	Disagree	-0,144	0,230	0,393	1	0,531
	Neither agree/disagree	-0,387	0,202	3,683	1	0,055
	Agree	0[a]			0	
Concerns about privacy online are exaggerated	Disagree	-0,642	0,197	10,632	1	*0,001*
	Neither agree/disagree	-0,428	0,241	3,154	1	0,076
	Agree	0[a]			0	
I feel I can control my privacy online	Disagree	-0,987	0,213	21,580	1	*0,000*
	Neither agree/disagree	-0,570	0,195	8,567	1	0,003
	Agree	0[a]			0	
On the Internet, it is safe to say whatever you think about politics	Disagree	-0,317	0,168	3,576	1	0,059
	Neither agree/disagree	-0,110	0,215	0,264	1	0,607
	Agree	0[a]			0	
The government should regulate the internet more	Disagree	-0,733	0,181	16,321	1	*0,000*
	Neither agree/disagree	-0,678	0,223	9,232	1	0,002
	Agree	0[a]			0	
There is no privacy, accept it	Disagree	0,196	0,166	1,384	1	0,239
	Neither agree/disagree	-0,568	0,215	6,970	1	0,008
	Agree	0[a]			0	

*a. This parameter is set to zero because it is redundant. *Missing values:435,86*

9 DISCUSSION AND CONCLUSIONS

The findings of our analysis indicate that people who state they have nothing to hide also believe that concerns about online privacy are exaggerated and they feel they can control their online privacy. That may lead to the tacit assumption that users' digital selves are likely to be surveilled, but if they have *nothing to hide*, then, this surveillance is not harmful. They believe in their 'innocence' so far so they are not guilty of collaborating with terrorists or committing cyber (or other) crimes; they also feel they can control their online privacy alone, but they need their governments to protect them. Therefore, this might indicate a partial

understanding of dataveillance: people who state they 'have nothing to hide' tend to project in their digital lives the same expectations they have from their governments in the physical world, to regulate the digital environment and protect them against violations that might occur e.g., either by corporate abuse of information power or attacks from cyber-criminals. We also showed that internet proficient respondents -in both the web and social media- are the ones who disagree with this statement, indicating that the demand for digital privacy does not entail having something to hide. We also discovered that people with higher digital skills believe internet privacy is within reach indicating that they do comprehend the inner mechanisms of the 'surveillance capitalism' but opt to manage them alone since they discard any further regulation on behalf of governments. This attitude is revealing of the dark colors with which governments have been painted due to surveilling practices they implemented in the name of security thus undermining their citizens' trust (Lyon 2003, 2014; Benkler, 2016), an issue much debated in virtue of the Covid-19 pandemic.

Does that mean that for a big part of our respondents dataveillance is accepted? Although comparative qualitative research is needed to thoroughly answer this question, it seems that peoples' assumptions about the violation of their digital privacy only go so far as to the acceptance that some companies may target them to and present them with advertisements that they will simply ignore. They may even think that they might be exposed to a few state officials and, since they are not guilty of hiding something, they should not be bothered if the exchange is the benefit of a free service or an online activity (Solove, 2007). In other words, '*I have nothing to hide*' seems to be derived from the comparative value of privacy over security. In an article published on Washington Post in 2005, judge Richard Posner was writing:

> 'collecting and processing data from machines cannot be considered a violation of privacy […]. Because of their huge volume, data is being 'sifted' by computers looking only for names, phones or addresses that may have some value for security reasons', whereas the machine keeps most of these data from being read by any intelligence officer' (Posner, 2005).

Bernal (2018: 71-77), however, argues against this '*myth of neutrality*', as the presumed innocence of the 'technical, automatic and passive' process performed by a network or an algorithm, ceases to be valid once the processing of the information leads to decisions and purposes that the original owner of the information does not control. People can be marginalized or become targets of algorithmic discrimination (Conrad, 2009; o' Neil, 2016; Noble, 2018) as important moments in their lives, such as being accepted to a university or receiving a loan can be determined based on profiles created by random online data (Helbing 2015: 7; O 'Neil 2016: 1; Eubanks 2018). Human lives are becoming more and more visible, while power asymmetries are becoming more invisible and, thanks to the growing establishment of complex data systems, are also becoming commonsensical (Lupton

2014). As a result, under the pretext of security, digital media do not contribute to the 'democratization of democracy' but rather to its destabilization when governments surveil citizens and corporations 'flesh them out' of streams of data to manipulate them and potentially modify their behavior (Foa & Mounk, 2017).

Users, quite justifiably, require protection in their digital lives as they are expected to deal with violations occurring on such high technological levels they don't even know exist: in our study the majority of the respondents state that they '*don't feel they can control their online privacy*'. However, the propagation of the '*I have nothing to* hide' attitude raises three problems. First, it assumes that privacy is about being able to hide something bad (Posner 1978; Schneier 2006; Bernal 2018). Second, it narrows down the debate on surveillance and exploitation of personal data to the irrelevant issue of whether one has something to hide and diverts it from the real questions which are, as Zuboff (2020) so aptly puts them, '*Who knows? Who decides who knows? Who decides who decides who knows*?' The third problem concerns the misconception of people who believe that, since they 'have nothing to hide', they will be permanently 'innocent' by neglecting the version in which their digital existence can be incriminated by anyone who might have an agenda. Shephard (2016) observes that when 'a person loses control of his information, he/she also loses control of the potential transformations of that information'. This is more likely to happen through 'surveillance assemblages' which 'datafy' aspects of identity, individuality and diversity (Poullet & Dinant 2006; Haggerty & Erickson 2000). If the challenge behind the claim '*I have nothing to hide*' is '*then you have nothing to fear*', that implies that 'good' people do not need privacy, as long as they have nothing to hide and 'bad' people do not deserve it, since obviously what they want to hide is harmful. Which reminds us of Zuboff's 'treacherous hallucination' that privacy is private. Within the confusing gap between what we know and what is known about us, we neglect that the very value of privacy is public - a collective good that is inseparable from the values of human autonomy and self-determination upon which privacy as well as citizenship depend (Weintraub & Kumar, 1997).

Therefore, **legislation and regulation** are firstly required in order to tackle the epistemic inequality. It is obvious that self-regulation of tech giants is coming to an end and state-based regulation and stronger enforcement of existing legislation is necessary. In Greece, the right to the protection of personal data is enshrined in the 2001 revision of Article 9A of the Constitution and is regulated by the General Rule for the Protection of Data (2016/679) which was enforced on May 2018 along with law 4624/2019 which defines the enforcement measures that integrated the European Directive (2016/680). However, according to the Special Eurobarometer 487a Survey[28], although Greek people seem coordinated with the rest of Europe concerning their knowledge about the existence of the General Data Protection Regulation, 39% of the respondents have not even heard which are the six rights GDPR protects landing them well below the European average. Which gives rise

[28] http://ec.europa.eu/commfrontoffice/publicopinion

to a second imperative: **information and digital literacy**. In Greece, as well as throughout Europe, the legal framework is set but people need to know their rights and the authorities that protect them. Enhancing informational channels about the legal status of peoples' online rights can only advance digital citizenship skills along with proper education. With Google in the lead, the top surveillance capitalists seek to control labor markets in expertise – including data science – eliminating competitors such as start-ups, universities, high schools, municipalities, established corporations in other industries or less wealthy countries. People need to familiarize themselves with the language of the digital world to the best of their abilities. If 20th century politics were defined by who owns the means of production, 21st century politics needs to be based on who owns the production of meaning. Introducing digital literacy in schools is of the utmost importance especially given the fact that children and teenagers today are digital natives that need to be best equipped in order to adapt to the even more complex and technically defined world of the future.

Although it is unfair for the users to carry once again the burden of securing their own privacy having to deal with technological savants behind algorithmic curtains, that is where a third imperative comes in: **algorithmic transparency through explainable AI.** One of the sections of the EU's General Data Protection Regulation (GDPR) focuses on the right to 'explanation'. Essentially, it mandates that users be able to demand the data behind the algorithmic decisions made for them including recommendation systems, credit and insurance risk systems, advertising programs and social networks. In doing so, it tackles 'intentional concealment' by corporations. However, the ambiguity and limited scope of the 'right not to be subject to automated decision-making' contained in Article 22 (from which the 'right to explanation' derives) raises questions over the actual protection provided to data subjects (Wachter et al., 2017). Furthermore, article 22 does not address the technical challenges associated with transparency in modern algorithms. Explainable AI (Miller, 2017; Pasquale, 2014; Edwards & Veale, 2017) is actually algorithms that can reveal how they work and why they end up in making a specific decision. Therefore, systems that work by analyzing and reporting which information input weighted the most in a decision-making algorithm, e.g., measuring and presenting how important the number of accidents a driver might have had in calculating the cost of their car insurance, may lift the veil over the 'man behind' the algorithmic 'curtain' …

FUNDING STATEMENT AND ACKNOWLEDGMENTS

This article is an output of the project "Research, Education and Infrastructures: the triangulation of EKKE strategic axes (REDI)", which is co-financed by the European Regional Development Fund in the framework of the Operational Programme "Competitiveness, Entrepreneurship and Innovation 2014-2020"

(EPAnEk). The authors thank the anonymous reviewers for their constructive suggestions for the article to take its final form.

REFERENCES

Acquisti, A., Taylor, C. & Wagman, L., 2016, "The Economics of Privacy". *Journal of Economic Literature* 54 (2): 442-92.

American Educational Research Association, January 2019, "Voter preference for Trump linked to bullying in middle schools". *ScienceDaily*. Retrieved April 2020, from www.sciencedaily.com/releases/2019/01/190109090917.htm

Amnesty international Report, 2019, 'Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights'. Retrieved January 2020 from https://amnestyusa.org/wp-content/uploads/2019/11/Surveillance-Giants-Embargo-21-Nov-0001-GMT-FINAL-report.pdf

Amoore, L., & De Goede, M., 2005, "Governance, Risk and Dataveillance in the War on Terror". *Crime, Law and Social Change* 43: 149-173.

Ariely, D. & Berns, G.S., 2010, "Neuromarketing: the hope and hype of neuroimaging in business". *Nature Reviews. Neuroscience*, 11(4): 284-292.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar M. & Turner, E., 2019, 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information', Pew Research Center. Retrieved February 2021 from: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Bauman, S., 2019, *Political Cyberbullying: Perpetrators and Targets of a New Digital Aggression*. Praeger

Benkler, Y., 2016, 'We cannot trust our government, so we must trust the technology', *The Guardian*, 22 February 2016. Retriever February 2021 from https://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi

Bernal, P., 2018, *The Internet, Warts and All. Free Speech, Privacy and Truth*. Cambridge University Press

Bond, R., Fariss, C., Jones, J. 2012, 'A 61-million-person experiment in social influence and political mobilization'. Nature 489: 295–298. https://doi.org/10.1038/nature11421

Boyd, D. and Crawford, K., 2012, Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15(5): 662-79.

Brown B., 2001, "Studying the internet experience". *Hp Laboratories Technical Report HPL* 49. Retrieved February 2020 from https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf.

Brunton, F. & Nissenbaum, H., 2015, *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT Press

Busvine, D. & Rinke, A, 2020, 'Germany flips to Apple-Google approach on smartphone contact tracing', Reuters, 26 April 2020. Retrieved February 2021 from https://www.reuters.com/article/uk-health-coronavirus-europe-tech-idUKKCN22807X

Bustos de, C.M. & Izquierdo-Castillo, L., 2019, "Who will control the media? The impact of GAFAM on the media industries in the digital economy". *Revista Latina de Comunicación Social* 74: 803-821.

Cammaerts, B., 2008, "Critiques on the participatory potentials of Web 2.0". *Communication, Culture and Critique* 1(4): 358-77.

Carrascal, J.P., Riederer, C., Erramilli, V., Cherubini, M., de Oliveira R., 2013, "Your browsing behavior for a Big Mac: economics of personal information online". In *Proceedings of the 22nd international conference on WorldWideWeb*, Rio de Janeiro, Brazil, 189–200.

Clarke, R. 1994, "Dataveillance by Governments: The Technique of Computer Matching". *Information Technology & People* 7(2): 46-85.

Conrad, K., 2009, "Surveillance, Gender, and the Virtual Body in the Information age". *Surveillance & Society* 6(4): 380–387

Crouch, C., 2004, *Post Democracy*, Polity, Cambridge

Curran, D., 2018, "Are you ready? Here is all the data Facebook and Google have on you". *The Guardian*, 30 March 2018. Retrieved March 2020 from https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy

Davenport, T. H. & Beck, J. C., 2013, *The Attention Economy: Understanding the New Currency of Business*. Cambridge, MA: Harvard Business Press.

Debatin, B., Lovejoy, J.P, Horn, A.K. & Hughes, B.N, 2009, "Facebook and online privacy: attitudes, behaviors, and unintended consequences". *Journal of Computer-Mediated Communication* 15(1):83 – 108

Demertzis, N., 2020, 'The pandemic as trauma' (Η Πανδημία Ως Τραύμα). In Γεωργακόπουλος, Θ (ed), Οι Ιδέες Της Πανδημίας-15 κείμενα για το πώς ο κορωνοϊός αλλάζει την Ελλάδα και τον κόσμο. διαΝΕοσις Publications, Athens

Demertzis, N. and Eyerman, R., 2020., "Covid-19 as Cultural Trauma". American Journal of Cultural Sociology, 8 (2): 428-450. DOI 10.1057/s41290-020-00112-z

Demertzis, N. & Tsekeris, C., 2018, "Multifaceted European Public Sphere – Socio-Cultural Dynamics". In B. Cammaerts, N. Anstead & R. Stupart, Media@LSE Working Paper Series. Media and Communications, Media@LSE, London School of Economics and Political Science.

Derikx, S., De Reuver, M., Kroesen, M., & Bouwman, H., 2015., "Buying-off Privacy Concerns for Mobility Services in the Internet-of-things Era: A Discrete Choice Experiment on the Case of Mobile Insurance". In

Proceedings of the 28th Bled eConference. Retrieved February 2020 from http://aisel.aisnet.org/bled2015/28

DeVellis, R. F., 2003, *Scale Development: Theory and Applications*. Thousand Oaks, CA: Sage.

Douzinas, K., 2020, 'The Biopolitics of the Pandemic' ('Η Βιοπολιτική της Πανδημίας'). In Π. Κ α π ό λ α, Γ. Κ ο υ ζ έ λ η ς & Ο. Κ ω ν σ τ α ν τ άς (Ε π ι μ) *Α π ο τ υ π ώ σ ε ι ς Σ ε Σ τ ι γ μ έ ς Κ ί ν δ υ ν ο υ*, Ε τ α ι ρ ε ί α ς Μ ε λ έ τ η ς τ ω ν Ε π ι σ τ η μ ώ ν τ ο υ Α ν θ ρ ώ π ο υ, Νήσ ο ς Publication, Athens

Draper, N. & Turow, J., 2019, 'The corporate cultivation of digital resignation'. New Media & Society 21(4), DOI: 10.1177/1461444819833331

Edwards, L. & Veale, M., 2018, 'Enslaving the algorithm: From a 'right to an explanation' to a 'right to better decisions?' IEEE Security & Privacy

Egelman, S., Felt, AP & Wagner, D., 2012, "Choice architecture and smartphone privacy: there's a price for that". In *Proceedings of the 11th annual workshop on the economics of information security*. Berlin, Germany.

Ellison, N.B., Vitak, J., Steinfield C., Gray, R. & Lampe, C., 2011, "Negotiating privacy concerns and social capital needs in a social media environment". In: *Privacy online*. Berlin Heidelberg: Springer, 19–32.

Eubanks, V., 2018, *Automating Inequality How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Publishing Group

European Commission Joint Research Centre Report, 2020, 'Technology and Democracy'. Retrieved February 2020 from https://ec.europa.eu/jrc

European Commission Special Eurobarometer 487a, 2019, The General Data Protection Regulation. Retrieved February 2021 from https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/1974/yearTo/2019/surveyKy/2222

Floyd, F. J. & Widaman K. F. (1995). Factor Analysis in the Development and Refinement of Clinical Assessment Instruments. *Psychological Assessment* 7(3): 286-299.

Flick, C., 2016, "Informed Consent and the Facebook Emotional Manipulation Stud". *Research Ethics* 12(1): 14–28.

Foa, R.S. & Mounk, Y., 2017, "The Signs of Deconsolidation". *Journal of Democracy* 28(1): 5-15.

Fuchs, C. 2012, "The Political Economy of Privacy on Facebook". *Television & New Media* 13(2): 139-159.

Fuchs, C. 2014, "Social Media and the Public Sphere', tripleC: Communication, Capitalism & Critique, *Journal for a Global Sustainable Information Society* 12(1): 57-101.

Gross, J.A., 2020, "Government okays mass surveillance of Israelis' phones to curb coronavirus". *Times of Israel*, 15 March 2020. Retrieved April 2020 from https://www.timesofisrael.com/government-okays-mass-surveillance-of-israelis-phones-to-curb-coronavirus/

Gould, W., 2000, "Interpreting logistic regression in all its forms". In: *Stata Technical Bulletin* 53: 19-29.

Haggerty, K.D. & Ericson, R.V., 2000, "The surveillant assemblage", *British Journal of Sociology* 51(4): 605–622.

Hayden, M., 2014, General Michael Hayden Beyond Snowden: An NSA Reality Check. *World Affairs* 176 (5): 13-23

Helbing, D., 2015, *Thinking Ahead—Essays on Big Data, Digital Revolution, and Participatory Market Society*. Springer

Helbing, D., 2020, The Corona Crisis Reveals the Struggle for a Sustainable Digital Future. TRAFO – Blog for Transregional Research, 21.05.2020, https://trafo.hypotheses.org/23989

Heller, C., 2011, *Post-Privacy: Prima leben ohne Privatsphäre*. München: Beck.

Hindman, M., 2009, *The myth of digital democracy*. Princeton, NJ: Princeton University Press.

Hsu T. & Celia Kang, C., 2018, "Demands Grow for Facebook to Explain Its Privacy Policies". *New York Times*, 26 March 2018. Retrieved March 2020 from https://www.nytimes.com/2018/03/26/technology/ftc-facebook-investigation-cambridge-analytica.html

Keyes, R., 2004, *The Post-Truth Era: Dishonesty and Deception in Contemporary Life*, St. Martin's Press

Kokolakis, S., 2017, "Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon". In *Computers & Security* 64: 122–134.

Kontiades, X., 2020, *Pandemic, Biopolitics and Rights – The World after Covid-19* (Πανδημία, Βιοπολιτική και Δικαιώματα – Ο κόσμος μετά τον Covid 19). Kastaniotis Publications, Athens

Kramer, A. D. I, Guillory, J. E, & Hancock J. T., 2014,' Experimental evidence of massive-scale emotional contagion through social networks'. PNAS 24: 8788-8790. https://doi.org/10.1073/pnas.1320040111

Kucklick, C., 2014, *Die granulare Gesellschaft. Auf dem Weg ins Zeitalter der Ungleichheit*. Berlin: Ullstein Buchverlage.

Laudon, K., 1997, "Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information". New York University Stern School of Business, Working Paper IS-97-4.

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): 862–77.

Lyon, D., 2001a, *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, D., 2001b, "Facing the Future: Seeking Ethics for Everyday Surveillance", *Ethics and Information Technology*, 3 (3): 171-180.

Lyon, D., 2014, "Surveillance, Snowden, and Big Data: Capacities, consequences, critique". *Big Data & Society*, 1-13.

Lyon, D., 2003, *Surveillance After September 1 1*(Themes for the 21st Century). Malden, MA: Polity

Madden, M., 2014, "Public perceptions of privacy and security in the post-Snowden era". Pew Research Center. Retrieved February 2020 from https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/

Mai, J. E., 2016, "Big data privacy: The datafication of personal information". *The Information Society* 32 (3): 192-199

Mayer-Schonberger, V. & Cukier, K., 2013. *Big data: A revolution that will transform how we live, work and think*, New York, NY: Houghton Mifflin Harcourt.

McIntyre, L., 2018, *Post Truth*, The MIT Press Essential Knowledge series

Miller, T., 2017, Explanation in artificial intelligence: insights from the social sciences. Retrieved February 2021 from https://arxiv.org/pdf/1706.07269.pdf.

Mosco, V., 2009, *The Political Economy of Communication*. London: Sage.

Murgia, M., 2019, 'Who's using your face? The ugly truth about facial recognition', *Financial Times*, 18 Sep 2019. Retrieved February 2021 from: https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e

Ngwenyama, O. & Klein, S., 2018, "Phronesis, Argumentation and Puzzle Solving in IS Research: Illustrating an Approach to Phronetic IS Research Practice". *European Journal of Information Systems* 27(3): 347-366

Nield, D., "All the Ways Google Tracks You—And How to Stop It". The Wired, 27 May 2019. Retrieved April 2020 from https://www.wired.com/story/google-tracks-you-privacy/

Noble, S.U., 2018, *Algorithms of Oppression How Search Engines Reinforce Racism*, NYU Press

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.

Norval, A., & Prasopoulou, E., 2017, 'Public Faces? A Critical Exploration of the Diffusion of Face Recognition Technologies in Online Social Networks". *New Media & Society* 19(4): 637-654.

O'Neil, C., 2016, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Books, New York.

OECD, 2019, *How's Life in the Digital Age? Opportunities and Risks of the Digital Transformation for People's Well-being*. Paris: OECD Publishing.

Papadoudis, G., 2018, "Multiple Discrimination and Inequalities: An Empirical Investigation". In *Tackling multiple discrimination in Greece*. ION Publishing Group & National Centre for Social Research, 213-233.

Pasquale, F., 2014, *The black box society: the secret algorithms that control money and information*. Cambridge: Harvard University Press

Park, Y.J., Chung, J.E & Shin, D.H., 2018, "The Structuration of Digital Ecosystem, Privacy, and Big Data Intelligence. *American Behavioral Scientist*, SAGE Publications, 1-19.

Peterson, A., 2013, 'Former NSA and CIA Director Says Terrorists Love Using Gmail,' Washington Post, September 15, 2013, retrieved February 2021 from https://www.washingtonpost.com/news/the-switch/wp/2013/09/15/former-nsa-and-cia-director-says-terrorists-love-using-gmail/ .

Posner, R., 1978, "The Right of Privacy". *Georgia Law Review* 12: 393-428.

Posner, R., 2005, "Our Domestic Intelligence Crisis", *Washington Post*, 21 Δεκεμβρίου 2005. Retrieved January 2020 from https://www.washingtonpost.com/archive/opinions/2005/12/21/our-domestic-intelligence-crisis/a2b4234d-ba78-4ba1-a350-90e7fbb4e5bb/

Poullet, Y & Dinant, J.M., 2006, "The internet and private life in Europe". In Kenyon, A. T. & Richardson, M., *New dimensions in privacy law: international and comparative perspectives*, Cambridge University Press, 60-90

Rosen, J., 2002, 'Total Information Awareness', 15 Dec 2002, The New York Times Magazine, retrieved February 2021 from https://www.nytimes.com/2002/12/15/magazine/the-year-in-ideas-total-information-awareness.html

Rule, J. B., McAdam, D., Stearns, L., & Uglow, D., 1983, "Documentary Identification and Mass Surveillance in the United States. *Social Problems* 31(2): 222-234.

Schneier, B., 2006, "The Eternal Value of Privacy". *The Wired*, May 18 Μαΐου 2006. Retrieved February 2020 from http://www.wired.com/news/columns/1,70886-0.html

Schuster, S., Van den Berg, M., Larrucea, X., Slewe, T., & Ide-Kostic, P., 2017, "Mass Surveillance and Technological Policy Options: Improving Security of Private Communications". *Computer Standards & Interfaces* 50: 76-82.

Sennett, R., 1993, *The Fall of Public Man*. London: Faber and Faber.

Shephard, N., 2016, "Big data and sexual surveillance". APC Issue Papers. Retrieved February 2020 from http://www.apc.org/sites/default/files/BigDataSexualSurveillance_0.pdf

Shorey, S. and Howard, P. N., 2016, "Automation, big data, and politics: A research review". *International Journal of Communication* 10(2016): 5032-55.

Singer, N. & Sang-Hun C., 2020, "As Coronavirus Surveillance Escalates, Personal Privacy Plummets". *The New York Times*, 23 March 2020. Retrieved April 2020 from https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

Smith, G. J. 2016, "Surveillance, Data and Embodiment: On the Work of Being Watched. *Body & Society* 22(2): 108-139

Smith, D., 2020, "Google keeps a frightening amount of data on you. Here's how to find and delete it". *Cnet*. 7 March 2020. Retrieved April 2020 from https://www.cnet.com/how-to/google-keeps-a-frightening-amount-of-data-on-you-heres-how-to-find-and-delete-it/

Solove, D. J., 2007, "I've got nothing to hide' and other misunderstandings of privacy". San Diego Law Review 44: 745

Solove, D., 2013, 'Privacy Self-Management and the Consent Dilemma', 126 Harvard Law Review 1880 . Retrieved January 2021 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018

Solove, D., 2020, 'The myth of the Privacy Paradox', GW Law School Public Law and Legal Theory Paper No. 2020-10. Retrieved January 2021 from https://ssrn.com/abstract=3536265

Spiekermann, S., Grossklags J. & Berendt B., 2001, "E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior". In *Proceedings of the 3rd ACM conference on electronic commerce*. Florida, USA, 38–47.

Spourdalakis, M., 2020, 'The post-coronavirus Democracy – Will it be socialistic or will it not exist?' (Η μετά κορωνοϊού - Δημοκρατία θα είναι σοσιαλιστική ή δεν θα υπάρχει). In Π. Καπόλα, Γ. Κουζέλης & Ο. Κωνστάντας (Επιμ) *Από τους πώσεις Στις Συγμές Κίνδυνου*, Εταιρεία Μελέτης των Επιστημών του Ανθρώπου, Νήσος

Srnicek, N., 2017, *Platform Capitalism*. Polity Press.

Stamouli, N., 2020, 'Coronavirus bundles Greece into the digital era'. Politico, 4 Feb 2020, retrieved February 2021 from: https://www.politico.eu/article/coronavirus-bundles-greece-into-the-digitalera/amp/

Steidl, P., 2012, *Neurobranding*. CreateSpace Independent Publishing Platform.

Stein. A., 2020, "How to restore data privacy after the coronavirus pandemic". *World Economic Forum*, 31 Mar 2020. Retrieved April 2020 from https://www.weforum.org/agenda/2020/03/restore-data-privacy-after-coronavirus-pandemic

Stutzman, F., Vitak J., Ellison N.B., Gray R., & Lampe C., 2012, "Privacy in Interaction: exploring disclosure and social capital in Facebook". In *Proceedings of the 6th international conference on weblogs and social media* (ICWSM 2012), Dublin, Ireland.

Taddicken M., 2014, "The 'privacy paradox' in the social web: the impact of privacy concerns, individual characteristics and the perceived social relevance on different forms of self-disclosure". *Journal of Computer-Mediated Communication* 19(2):248–73.

TRUSTe, 2014, US Consumer Confidence Privacy Report Consumer Opinion and Business Impact. Retrieved February 2020 from http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

Tsekeris, C., & Katerelos, I. (eds), 2014, *The social dynamics of Web 2.0: Interdisciplinary perspectives*. London: Routledge.

Tsekeris, C., Demertzis, N., Linardis, A., Iliou, K., Kondyli, D., Frangiskou A. & Papaliou, O., 2020, Investigating the Internet in Greece: findings from the World Internet Project. Hellenic Observatory Discussion Papers on Greece and Southeast Europe, no 153

Tzarelas, D., 2020, 'The Return of the State in the midst of the pandemic' ('Η επιστροφή του κράτους εν μέσω πανδημίας'). In Π. Καπόλα, Γ. Κουζέλης & Ο. Κωνσταντάς (Επιμ) *Από τους πώσες ις Σε Σ τι γμές Κίνδυνου*, Ετα ιρεία Μελέτης των Επιστημών του Ανθρώπου, Νήσος Publications, Athens.

Tzogopoulos, G. N., 2020, "The Internet in the Coronavirus Era, *The Begin Sadat Center for Strategic Studies*, 30 March 2020. Retrieved April 2020 from https://besacenter.org/perspectives-papers/coronavirus-internet/

van der Schyff, K., Krauss, K.E.M. & Kroeze, J.H., 2018, "Facebook and Dataveillance: Demonstrating a Multimodal Discourse Analysis", *Twenty-fourth Americas Conference on Information Systems,* New Orleans

van Dijck, J. 2014, "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society* 12(:2): 197.

van Dijck, J., 2013, *The Culture of Connectivity: A Critical History of Social Media*, Oxford: Oxford University Press.

Wachter, S., 2020, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising'. Berkeley Technology Law Journal, Vol. 35:2

Wachter, S., Mittelstadt, B. & Floridi, L., 2017, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation'. International Data Privacy Law 7-2: 76–99, https://doi.org/10.1093/idpl/ipx005

Watson, C., 2018, "The key moments from Mark Zuckerb'rg's testimony to Congress. *The Guardian*, 11 April 2018. Retrieved February 2020 from https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments

Weintraub, J. & Kumar, K. (eds.) 1997, *Public and Private in Thought and Practice. Perspectives on a Grand Dichotomy.* Chicago: The University of Chicago Press.

Worthington, R. & Whitaker, T., 2006, "Scale Development Research-A Content Analysis and Recommendations for Best Practices". The Counseling Psychologist 34 (6): 806-838

Wouters, C., 2007, *Informalization: Manners and emotions since 1890*. London: Sage

Zafeiropoulou, A.M, Millard, D.E, Webber, C & O'Hara, K., 2013, "Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?". In: Proceedings of the 5th annual ACMWeb Science Conference, May 2–4, Paris, France

Zuboff, S., 2019, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, PublicAffairs, New York.

Zuboff, S., 2020, 'You Are Now Remotely Controlled', *The New York Times*, 24 Jan 2020. Retrieved February 2020 from https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html

Zuboff, S., 2021, 'The Coup We Are Not Talking About', *The New York Times*, 29 Jan 2021. Retrieved February 2021 from https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html

Zurawicki, L. (2010). *Neuromarketing: Exploring the brain of the consumer*. London: Springer.