MEDIATIZATION STUDIES 1/2018 DOI: 10.17951/ms.2018.1.2.49-68

GRZEGORZ PTASZEK

AGH University of Science and Technology, Kraków, Poland

gptaszek@gmail.com

Surveillance capitalism and privacy. Knowledge and attitudes on surveillance capitalism and online institutional privacy protection practices among adolescents in Poland

Abstract. The purpose of the study was to determine the level of knowledge and attitudes towards surveillance capitalism and online institutional privacy protection practices among adolescents in Poland (aged 18–19), as well as to determine the relationships between these variables. Surveillance capitalism has emerged as a result of internet users' activities and involves the collection of all data about these users by different entities for specific benefits without letting them know about it. The dominant role in surveillance capitalism is played by hi-tech corporations. The aim of the study was to verify whether knowledge, and what kind of knowledge, on surveillance capitalism translates into practices related to the protection of online institutional privacy. The study was conducted on a sample of 177 adolescents in Poland. The main part of the questionnaire consisted of two scales: the scale of knowledge and attitudes on surveillance capitalism, and the scale of online institutional privacy protection practices. The results of the study, calculated by statistical methods, showed that although the majority of respondents had average knowledge and attitudes about surveillance capitalism, which may result from insufficient knowledge of the subject matter, this participation in specialized activities/workshops influences the level of intensification of online institutional privacy protection practices.

Keywords: institutional privacy, surveillance capitalism, Polish adolescents, online privacy protection practices

Introduction

In the digital era, digital data is a valuable resource. Companies collect, store, analyze and commodify it, often without the approval of those from which the data is collected. The phenomenon is known as "traceability" (Latour 2007) and indicate that each of our online moves is tracked and enters a database to be analyzed in the

future. Traceability is now an inseparable element of digital culture and our participation in it. Many researchers dealing with data (Clark 2006; Ashworth, Free 2006; Degli Esposti 2014; van Dijck 2014) underline that commercial data collection is a new form of surveillance defined as dataveillance (van Dijck 2014) or surveillance capitalism (Zuboff 2015, 2019). The researchers observed that digital data can be analyzed by algorithms for commercial or political outcomes to foresee successfully sexual orientation (Jernigan, Mistree 2009), gender, ethnic origin, political views, and religion (Kosinski, Stillwell, Graepel 2013), and also for a political profiling (Nadler, Crain, Donovan, 2018).

Many privacy researchers focus on the sharing of personal information (e.g. gender, age, address, personal photos etc.) and the self-disclosure of the same on social media sites (Barnes 2006; boyd, Hargittai 2010; Debatin et al. 2009; boyd 2014; Taddicken 2014; Culver, Grizzle 2017). They concentrate on social privacy in networked public spaces, especially in relation to other users (e.g. parents, classmates, unknowns). But there are few researches concerned with privacy in the context of collecting and analyzing digital data, especially for selling it or predicting users' private traits or preferences (Turow, Feldman, Meltzer 2005; Raynes-Goldie 2010; Young, Quan-Haase 2013; Lutz, Ranzini 2017), what is called instutitional privacy (Raynes-Goldie 2010).

In this context, it is interesting to determine how many modern teenagers actually prefer to have access to content and digital products that protect their private data against surveillance capitalism practices, what knowledge they possess about the functioning of hidden algorithmic mechanisms violating their private sphere without their approval, and what protective strategies they have undertaken against surveillance capitalism. The purpose of the study was to determine the knowledge and attitudes on surveillance capitalism possessed by youths in Poland aged of 18–19 years, and whether this relates to online privacy protection practices. For many years, Internet users in Poland have been at the international forefront when it comes to use online applications for blocking online advertising (Newman et al. 2017, p. 26, Digital in 2018, p. 47). They are also characterized by a very low level of digital optimism, or the belief that new technologies offer more opportunities then risks. In 2018, in the Digital study, they occupied third place (41%) just behind Belgians (38%) and Germans (37%). In connection with the above, one might assume that they have high knowledge about different surveillance and online protection privacy practices.

An online questionnaire was created to investigate how adolescents in Poland relate to knowledge and attitudes on surveillance capitalism (KASC), and whether they undertake online institutional privacy protection strategies (IPPP).

The main research questions involved determining what young people in Poland know about the indications of surveillance capitalism, what attitudes they reveal about this, and what protective practices they prefer to protect against institutional privacy?

Surveillance capitalism in the age of Big Data

Modern technological infrastructure, from cookies through devices, online and mobile services to search engines and platforms, were designed to generate digital data that can be read algorithmically (Urichio 2011). As a consequence, the availability of a large amount of digital data combined with the improved computational technology of their processing (data mining), largely derived from research on artificial intelligence, has enabled the effective datafication of social, cultural and political life on a wide scale and started a socio-cultural phenomenon called Big Data. Thanks to various applications installed in smartphones, companies know how long we sleep, what activities we undertake during the day, how much time we devote to commuting to work, school and home, what we like, how we spend our free time, what interests we have, etc. Big Data provides a lot of different kinds of data that can be combined, compared and correlated in any way. At the same time this is both a significant value and weakness of Big Data. Since the majority of our professional and private activities are carried out using various digital devices, Big Data covers a broad range of our everyday activities. The more frequently we use digital devices, the more identifiable we become.

As Shoshana Zuboff notes, Big Data is now the basis of a new logic of capital accumulation, which she calls "surveillance capitalism". Surveillance capitalism "determines what is measured, and what is passed over; how resources and people are allocated and organized; who is valued in what roles; what activities are undertaken – and for what purpose. The logic of accumulation produces its own social relations and with that its conceptions and uses of authority and power" (Zuboff 2015, p. 77). Surveillance capitalism is a "new form of information capitalism [that] aims to predict and modify human behavior as a means to produce revenue and market control" (Zuboff 2015, p. 75). As Zuboff notes, surveillance capitalists quickly realized that the most valuable data is generated when consumers are pushed or forced into specific behaviors that bring profit to companies and therefore their automated machine processes not only follow our behavior but also shape it (Zuboff 2019, p. 18).

In case of surveillance capitalism, digital data is collected to not specifically defined goals that are unknown to a consumer (Lyon, Bauman 2013; van Dijck 2014, p. 205). As Debatin et al. notices what is visible (and what he is conscious) is only a small part (1/8) of the activities and network interactions. The whole rest (7/8) makes the sphere invisible, hidden, which consists of "data that trickle down from the interactions and self-descriptions of the users in the visible part. To maintain the separation (and the user's motivation to provide and constantly update his or her personal data), any marketing and advertising based on these data must be unobtrusive and subcutaneous" (Debatin et al. 2009, p. 88). The value of the data is not defined by their acquisition itself, but by the potential use in the future and the possibility of their unlimited use (Mayer-Schonberger, Cukier 2013). Moreover, data monitoring far exceeds any

watching of individuals, because it penetrates deeply into social issues (Andrejevic 2012, p. 86) in order to predict complex phenomena such as consumers' decisions (Nissenbaum 2010, pp. 42–44; Citron, Pasquale 2014).

Surveillance capitalism is part of the struggles of new media corporations looking to achieve hegemony in the communication networks, and is a basic business model of not only such technology giants as Google or Facebook, but also of various start-ups offering services and online applications. This hegemony is based on the asymmetry of relationship and information (Ramesh, Fish 2017; Nissenbaum 2010; Halavais 2009; Andrejevic 2014). Mark Andrejevic (2014) calls this asymmetry of the relation between those who collect, store and exploit large amounts of data, and those from whom this data is sourced, the big data divide. Each of these two groups has different options on the access and use of the data, which also determines the asymmetry of the relation (e.g. social sorters versus social "sortees", and forecasters versus those subordinating to the forecast). Moreover, Andrejevic notes that "the big data paradigm challenges the empowering promise of the Internet by proposing the superiority of post-explanatory pragmatics (available only to the few) to the forms of comprehension that digital media were supposed to make more accessible to the many" (Andrejevic 2014, p. 1675). danah boyd and Kate Crawford (2011) speak in a similar way, and in their opinion the present Big Data ecosystem creates a new kind of digital divide between the Big Data rich and the Big Data poor (boyd, Crawford 2011). In addition, David Lyon raises: "the overall effects of consumer surveillance, especially through all kinds of internet use, are not only to cream off those contented consumers and promise further rewards and benefits, but also to cut off those who do not conform to expectations" (Lyon, Bauman 2013, p. 104–105). A new form of digital exclusion is revealed based on the interests of those technological corporations which offer their services and products "for free". Users are aware of it, so they partly relinquish their privacy and agree to various forms of surveillance of their data, which simultaneously separates them from the threat of digital exclusion.

The asymmetry of information relies on controlling:

- all information about the user's activities on the Internet, social networking sites or mobile devices,
- information about the purposes and means of collecting, storing, analyzing and using the data and information that are collected about users,
- available information, making its selection dependent on intelligent algorithms analyzing user behaviors and preferences.

Surveillance capitalism should also be seen as a new form of "data colonialism" normalizing the exploitation of human beings through data and "paving the way for a new stage of capitalism whose outlines we only glimpse: the capitalization of life without limit" (Couldry, Mejias 2018). In a situation where our behavior as consumers of the digital products and services offered by digital companies becomes what drives

surveillance capitalism and provides profits only to these companies (Zuboff 2019, p. 11), this phenomenon should be carefully analyzed in the context of institutional privacy and the protection practices against it.

Privacy in surveillance capitalism

In recent years, privacy in the digital era and in surveillance capitalism has been one of the most important issues. Surveillance of a user's online activity is very commonly identified as a restriction or interference with the right to privacy (UNESCO 2015). Privacy is important not only because it is an inalienable human right to protect one's identity, but also because it is a part of the structure of social life (Blank, Bolsover, Dubois 2014, p. 4). According to Nissenbaum: „Activities online, mediated by the Net, are deeply integrated into social life: they may be continuous with brick-and-mortar correlates or, at the very least, have the power to affect communications, transactions, interactions, and activities in those realms (and vice versa)" (Nissenbaum 2011, p. 38).

Academics in previous studies focused more on social privacy protection practices (controlling access to personal information on social media platforms for the other users) rather than institutional privacy protection practices (controlling how digital companies and their partners might use personal and digital data) (Raynes-Goldie 2010). Many researchers have noted that users are concerned about their privacy on the web, but they are practically unable to take any action to protect it. This variance between attitudes and behavior was defined as the "privacy paradox" (Barnes 2006; Acquisti, Gross 2006; Taddicken 2014). Blank, Bolsover, and Dubois (2014, p. 15–16), however, point out that this was indeed often the case at the beginning of SNS development, but now young users aged 14–24 are not apathetic toward online privacy. In turn, Taddicken (2014, p. 266) shows that there is no significant relationship between online privacy concerns on self-disclosure behavior, wherein she did not distinguish between public self-disclosure and self-disclosure behavior with clearly defined communities where users feel safe from privacy invasion. However, Trepte et al. (2014) argues that disparities between attitudes and behaviors might not indicate paradoxical and inconsistent behavior, but address different dimensions of privacy. His research shows that attitudes are not easy to use as predictors of privacy behavior, because there is more influence for this behavior due to negative online experiences and internet skills[1]. Similar conclusions follow from the research of Büchi et al. conducted among Swiss university students, where it was observed that "attitudes are not the primary explanation for users' varying levels of privacy protection", but online privacy breaches and skills. Participants who have experienced privacy violation online will engage in more self-protective privacy

[1] The authors consider the problem only for informational, social, and psychological privacy. They did not deal with institutional privacy.

behaviors (Büchi, Just, Latzer 2016, p. 16). It seems, however, that the situation in which there is a breach of privacy due to the action of a real person is more frequent and easier to observe than when users experience a breach of privacy due to the use of their data without their knowledge and approval, such as for sale to other entities or for profiling. Scandals such as that of Cambridge Analytica in 2018 occur extremely rarely, and, as demonstrated by the practice, did not translate into a massive outflow of Facebook users. What's more, profiling, and especially algorithmic personalization of content, can be perceived by users as beneficial, especially by those who do not have the motivation or the skills to personalize the content to their own preferences (Sundar, Marathe 2010). A factor that seems to play a significant role here involve the social benefits that users derive from disclosing information about themselves (Trepte et al. 2014, p. 8) which is rewarding for the user's brain (Tamir, Mitchell 2012).

Due to the debatable issue of the existence of the "privacy paradox" and the complexity and multi-dimensionality of online privacy behaviors, alternative proposals by researchers explain the discrepancy between privacy attitudes and real behavior as "privacy cynicism" (Hoffmann, Lutz, Ranzini 2016) or the "privacy dilemma" (Matzner et al. 2016).

The distinction for social privacy and institutional privacy seems to be crucial to explain how users more likely to undertake protection practices against other users than against invisible and abstract web actors. According to the Eurobarometer e-Privacy survey carried out among the population of the European Union aged 15–24, only slightly negative attitudes to tracking online activities prevail. For example, only 54% respondents think that their online activities monitored in exchange for unrestricted access to a certain website is not acceptable and 58% say that is unacceptable for companies to share information about them without their approval, even if it helps these companies to provide new services they might like. What is interesting is that a significant number of respondents allow such activities, with 45% stating that having their online activities monitored in exchange for unrestricted access to a certain website is acceptable, while 42% think that is acceptable for companies to share information about them without their approval, even if it helps these companies to provide new services they might like (European Union, DG COMM 2016, p. 57–59). From the research by Young and Quan-Haase, students who use Facebook showed little or no concern about threats from Facebook or third party data companies, but they were concerned about how other people may use personal data and information (Young, Quan-Haase 2013, p. 493–494). Users of Tinder were more concerned about institutional privacy then social privacy (Lutz, Ranzini 2017).

Importantly, online privacy researches indicate that there is a significant link between internet and digital skills (boyd, Hargittai 2010; Litt 2013), knowledge (Matzner et al 2016, pp. 282–285, Nissenbaum 2011, p. 45), and the intensity and the type of undertaken privacy practices. Some media scholars observe that the key to protecting our data is digital literacy. For example, Kennedy et al. believes that the 'conscious

user' of digital media education is becoming more and more important nowadays (Kennedy, Poell, van Dijck 2015), which means that awareness of how much users know about data streams and their abilities to control them is really important to manage privacy. This is confirmed by the studies (Büchi et al.) showing that internet skills are an important complementary predictor of self-protective privacy behavior (Büchi, Just, Latzer 2016, p. 15–16). As Matzner et al. concludes, protection of social privacy requires different practices and activities then institutional privacy (Matzner et al. 2016).

Methodology and hypotheses

The study tests two research hypotheses that concern two factors (attitude and skills), as discussed above, and how they influence the privacy behaviors:

1. Users with extensive knowledge and a negative attitude towards surveillance capitalism undertake online institutional privacy protection practices (IPPP).
2. Users participating in classes or workshops on internet safety and privacy (ISP) are much more likely to undertake online institutional privacy protection practices (IPPP).

In order to study how young Poles refer to surveillance capitalism, and whether they undertake related online institutional privacy protection strategies, an online questionnaire was created. The study was conducted in the period December 2017 – March 2018 among high school students and technical schools students aged 18–19 (N=177). Due to the selection of the sample, it was not representative.

The selection of the research group resulted from several factors. First of all, the 18–19 year-olds belonged to groups that use the Internet (54% daily or almost daily) and social media (40% daily or almost daily) most actively. Secondly, the 18–19 year-olds were in a formal stage of education.

The questionnaire consisted of 4 parts:

1) A statistical part/specifications (e.g. questions about age, gender, type of school, participation or non-participation in workshops on internet safety/digital literacy);
2) 5 questions regarding the use of digital devices and applications;
3) 33 statements verifying knowledge and attitude towards surveillance capitalism (KASC), e.g. "The websites I use have the right to collect private information about me", "Internet search engines, e.g. Google, Bing, Yahoo! Baidu records and stores the search terms", "Facebook is able to predict my emotions", "Based on online activity, someone can predict sexual orientation", "On the basis of online activity, companies create consumer profiles to which they direct personalized advertising", "If it is possible to sell private digital data in the future, I will be

happy to use it", "In the information society, data collected by technology companies can only be used to improve the devices or applications we use";

4) 30 statements verifying online institutional privacy protection practices (IPPP), e.g. "In an information society, data collected by technology companies can only be used to improve the devices or applications we use", "When I do not use the navigation or map function, I disable geolocation on a mobile device or social networking site", "I share my data on social networks with the number of steps or kilometers traveled and heart rate levels", "I use various search engines to protect my digital identity", "By logging into new websites using social media accounts, I check what permissions the page requests".

In the case of conclusions verifying knowledge and attitude, the respondent had to indicate answers on a 5-point Likert scale from "strongly disagree" to "strongly agree". In the case of conclusions verifying practices, the respondent had to indicate answers on a 5-point Likert scale from "never" to "all the time".

Because the essence of surveillance capitalism is the collection and use of the users' data by technological corporations in order to achieve their business goals, parts 3 and 4 include in the questionnaire issues concerning:

- Understanding how data is collected,
- Attitudes towards data collecting,
- Understanding the effects of surveillance capitalism,
- Application and privacy policy,
- Protecting against surveillance capitalism.

Participation by the respondents was voluntary and everyone consented to the processing of collected data for scientific purposes. The questionnaire was published online and a link to it was sent out along with an invitation to participate in the survey to teachers, based on the snowball method (subsequent teachers were to invite the next ones).

The study adopted explanatory variables: (1) participation in classes or workshops on ISP (yes/no), and variables explained: (1) knowledge and attitude on surveillance capitalism (KASC)[2], (2) online institutional privacy protection practices (IPPP)[3] and co-occurring variables: (1) knowledge and attitude on surveillance capitalism, and (2) online institutional privacy protection strategies.

In the statistical analysis of the obtained results, descriptive methods and methods of statistical inference were used. To characterize the average value for quantitative traits, the arithmetic average (*M*) was calculated, and the standard deviation (*SD*) was assumed to be the scattering pattern, while the quartile measure (*Q1, Mdn, Q3*) was

[2] The scale of knowledge and attitudes: totality of statements: 1–33 (including inversely scored 1, 4, 9, 10, 11, 19, 21, 23, 24, 25) (∑=165 points).

[3] The scale of practices: totality of statements 1–8, 12–19 (statement 17 is inversely scored) (∑= 80 points).

used to represent the position of the observation. The analysis of qualitative variables was performed by calculating the number and percentages of the occurrences of each value. The conformity of the distributions of quantitative traits with normal distribution was assessed using the Kolmogorov-Smirnov test (for $N > 100$) or Shapiro-Wilk (for $N < 100$) and on the basis of analysis of skewness and kurtosis indices as well as standard errors, on the basis of a visual assessment of their histograms, and QQ charts.

Due to the lack of conformity of variable distributions coexisting with the normal distribution to the study of compounds, Spearman's rank correlation was applied. To compare the distributions of quantitative variables in two groups, a Mann-Whitney U test was used (for variables with a non-normal distribution) or a Student's t-test for independent samples (for variables with near-normal distribution). The Levene test was used to determine the equality of variance in the samples. For all analyses, the maximum admissible type I error $\alpha = 0.05$ was assumed, while $p \leq 0.05$ was considered statistically significant.

Results

A. Characteristics of the studied group

A total of 177 people, high schools students and users of digital media, took part in the survey. The majority of respondents were 18 year-olds, at around 60%, while the remaining 40% were 19-year olds. Among the respondents, 51% attended a high school, while 49% attended a technical school. Almost two-thirds of the respondents (62%) were men, while over a third (38%) were women. The largest group of respondents involved people living in rural areas (38%).

Among the digital devices that the respondents indicated as the most frequently used, smartphones appeared in first place (100% of respondents), laptops in second place (70%), and desktop computers in third place (62%). Tablets (20%) were the least frequently used devices.

In the case of a number of applications installed on a smartphone, 40% of respondents indicated the "6–10" range for the application, while 15% indicated the range "11–15" and "above 20". Due to the fact that a tablet is not one of the popular devices used by the respondents, the most common indication for the number of applications installed on this device was the range "0–5" (20%).

The surveyed group was diverse in terms of experience and participation in classes or workshops on *internet safety and privacy* (ISP) conducted outside school or at school by people unrelated to school. Among the respondents, 51% did not participate in classes/workshops ISP, while 49% confirmed their participation in such activities.

Since almost 50% of the respondents participated in classes or workshops on ISP, it should be assumed that their knowledge about surveillance capitalism is high. Of

course, such an assumption has some limitations. Firstly because it is not known which issues were discussed during the classes/workshops, and secondly in what form they actually took place. These two factors may have a significant impact on the way knowledge is acquired.

Knowledge and attitude on surveillance capitalism (KASC)

The lowest level of KASC of the respondents was 62 points, while the highest one was 154 points. A result on this scale in the range of 132–165 points means great knowledge and a negative attitude towards surveillance capitalism (Tab. 1).

Table 1. Characteristics of the level of the KASC in the studied sample (N = 177)

Variable	*n*	*M*	*SD*	*Min*	*Max*	*Skew*	*K*	*K-S*	*p*
Knowledge and attitude on surveillance capitalism (KASC)	177	126,85	15,15	62	154	-0,98	2,14	0,09	0,002

Remark: *n* – number; *M*- average; *SD*- standard deviation; *Min* – lowest value; *Max* – highest value; *Skew* – skewness;

K – kurtosis; *K-S* – result of Kolmogorov-Smirnov test; *p* – significance level for the K-S test.

In "knowledge and attitudes" scale only 0.56% of respondents (one person) obtained a result showing very low knowledge and an extremely positive attitude toward surveillance capitalism, while about 40% of respondents (N = 71) obtained a score between 132–165 points, signifying a negative and definitely negative attitude towards surveillance capitalism as well as a very large and extensive knowledge on this subject. The highest number of respondents, 59.32% (N = 105), gave a result between the extreme scale of values (M=126.85, SD= 15.15).

The analysis of individual answers, however, yields interesting results. Although the vast majority of respondents fairly and fully agree that the internet should not be controlled either by governments (66.10%) or corporations (68.36%), a large number of them having no opinion on these issues (about governments – 17.51%, about corporations – 20.34%). The same applies to the online privacy at stake. But, almost 50% respondents fairly and totally agree that data collected by tech companies can be used to improve the devices or application, and 30.51% have no opinion on this issue. A large group of respondents (41.78%) fairly and completely agree that the websites have a right to collect private information about them, but a similar group (38.42%) does not agree. A total of 25% likes the fact that websites suggest products that may be of interest. Some of them declared forgoing from online privacy in exchange for free access to digital content (16.38%), but the large group has no opinion on this issue (22.6%). However, the vast majority of respondents would not sell private digital data in the future (55.37%) or would not exchange it for cheaper or free services (54.24%).

Knowledge and attitudes towards tracking and collecting user data are much more diverse than one might think, given the fact, that most adolescents strongly agree, and agree that each online activity or on a mobile device leaves a permanent footprint (87.5% of respondents).

When it comes to knowledge about the use of data by entities that collect and analyze them, that big group of adolescents strongly agree and agree, that companies collecting digital data can use programs to predict behaviors of online users (72%), but almost 21.5% adolescents neither agreed nor disagreed. The same number of survey participants strongly agreed, and agreed that mobile devices should collect data to determine the frequency, time, place and period of use by a user (72%), but 10% of adolescents had no opinion about this issue. 56% of the respondents thought that search engine results were complete and objective, although 25% neither agreed nor disagreed. In the case of knowledge by adolescents about the potential for using data for predicting personal trails or preferences, 38.41% strongly disagreed, and disagreed that Facebook was able to predict emotions, but a large group thought differently (31.64%), while 29.94% neither agreed nor disagreed. Significantly differing points of view were presented by respondents in terms of predicting preferences based on online activity. Here, 76.84% of the respondents strongly agreed, and agreed that it was possible. Over half of the respondents also agreed that the following could be predicted based on digital data: conscientiousness and openness (53%), gender (67%), sexual orientation (67%), economic status (59%), and political preferences (70%). Still, a large number of respondents had no opinion about the possibility of predicting personal characteristics based on online activity, i.e. conscientiousness and openness (20%), gender (16%), sexual orientation (21%), economic status (25%), and political preferences (20%).

Due to the large number of responses indicating a lack of knowledge and opinions, people participating in extracurricular activities or workshops on online security and privacy conducted by non-school personnel were checked if they differed from those who did not participate in such classes, in terms of the level of knowledge and attitudes about the online collection of data. Table 2 shows the results obtained in the study.

The Mann-Whitney U test analysis did not show statistically significant differences between the groups in the range of the tested variable: $Z = 1.64$, ni. This means that those who participated in extracurricular activities or workshops conducted by non-school people on online safety and privacy did not differ from those who did not participate in such classes, in terms of level of knowledge and attitudes about online data collection. The lack of a clear difference between groups may result from the lack of the subject of data protection and practices related to their collection and use during classes about internet safety and privacy, which was not tested in the study. In summary, the knowledge and attitudes of users about surveillance capitalism are diverse. Although the vast majority of adolescents agrees with the statement that their online privacy is at risk and is aware of the fact that any online activity leaves footprints

Table 2. The characteristic of knowledge and attitude level on surveillance capitalism among adolescents participating (n = 87) and non-participating (n = 90) in workshops about internet safety and privacy – Mann-Whitney U test

Variable	Internet safety and privacy (ISP) classes or workshops attendance	*n*	$\bar{r}$	*R*	Q_1	*Mdn*	Q_3	*M*	*SD*	*Min*	*Max*	*Z*	*p*
Knowledge and attitude on surveillance capitalism (KASC)	Yes	87	95.41	8301	122	129	138	128.11	16.45	62	154	1.64	0.101
	No	90	82.80	7452	117	127	135	125.63	13.75	92	151		

Remark: *n*- number, r̄ – average weight, *R* – total weight, Q_1 – 1st quantile, *Mdn* – median, Q_3 – 3rd quantile, *M* – average, *SD* – standard deviation, *Min* – lowest value, *Max* – highest value, *Z* – result of Mann-Whitney U test, *p* – significance level of *Z-test*

that can be used for different purposes, there is quite a large group of young people who do not have an opinion on such an important for their online privacy matters.

B. Online institutional privacy protection practices (IPPP)

The average level obtained by the respondents in the scope of IPPP was *M*=126.85 points with a standard deviation *SD*=15.15 point. On the other hand, the lowest level of IPPP among the respondents was 20 points, while the highest was 69 points; the average level obtained by the respondents in the scope of data protection practices was *M*=41.66 points with a standard deviation *SD*=9.27 points. The result on this scale in the range of 64–80 points means high and very high level of online privacy protection strategies.

Table 3. Characteristics of the level of the IPPP in the studied sample (N = 177)

Variable	*N*	*M*	*SD*	*Min*	*Max*	*Skew*	*K*	*K-S*	*p*
Online institutional privacy protection practices (IPPP)	177	41.66	9.27	20	69	-0.18	-0.28	0.08	0.005

Remark: *N* – number; *M*- average; *SD*- standard deviation; *Min* – lowest value; *Max* – highest value; *Skew* – skewness; *K*- kurtosis; *K-S* – result of Kolmogorov-Smirnov test; *p* – significance level for the K-S test.

As for the results on the "practice" scale, only 0.56% of the respondents (one person) obtained a result indicating a high degree of information privacy protection practices, 19.77% (N=35) presented a very low or low level; however, as much as 79.66% (N=141) obtained a result showing a moderate degree of privacy practices (between 33–64 points) (M=41.66, SD=9.27).

A significant number of respondents without a moderate level of intensification of practices may result from a lack of knowledge about surveillance capitalism and competence in privacy management (Fig. 1), especially those purely technical, connected for example with the ability to change application settings, as well as lack of tools for obfuscation activity (Fig. 2). In the part of literature review it was indicated that digital competences are an important complementary predictor of self-protective privacy behavior (Litt 2013; Büchi, Just, Latzer 2016, p. 15–16).

Although the vast majority of the adolescents turn off geolocalisation when they do not use it (47%), a large group of them still does not modify default setting after installation (17.51%) and 18.64% seldom modifies it. A large group also does not verify (12.53%) or seldom verifies (22.6%) the author and the source before uploading it.

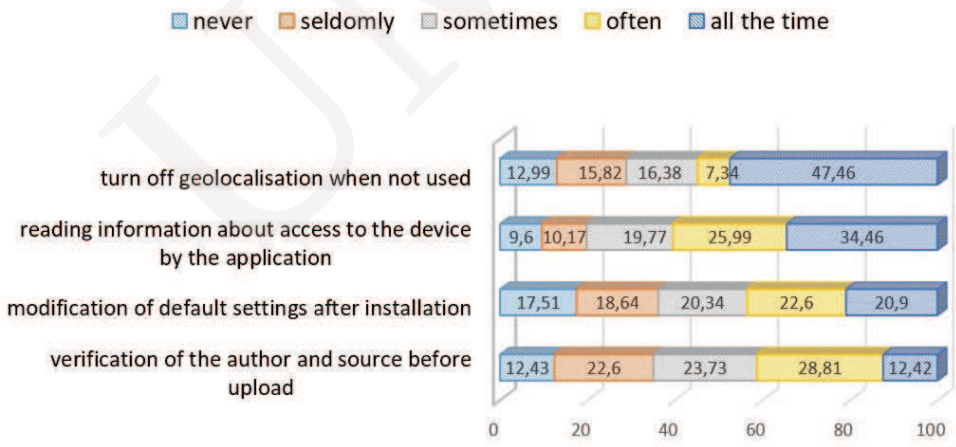

Figure 1. Online information privacy protection practices: setting of device and application [%], N=177.

The respondents do not use or seldom use light obfuscation practices (Fig. 2). A large group of respondents does not use different browsers (41%) as well as does not install plug-ins against tracking, e.g. Ghostery (40.68%). There are still respondents who do not delete cookies browser (22.03%) or do it seldomly (25.99). Moreover, a large number of respondents do not use a private browser mode (22.6%) or do it rarely (23.16%). Besides, many users do not log in at all (22.03%) or do so rarely (28.25%) to new websites using a social media account ("linking accounts").

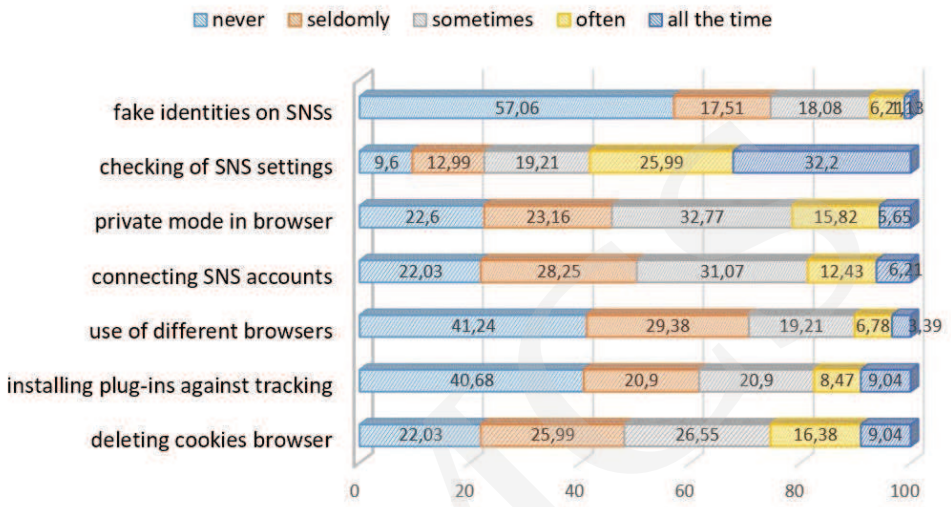

Figure 2. Online institutional privacy protection practices: light obfuscation [%], N=177.

To sum up, adolescents in terms of their privacy protection practices against the use of their data by institutions for various purposes are characterized by large diversity. While some practices are undertaken often or almost all the time by almost half of the adolescents (e.g. turn off geolocalisation when not used, checking of SNS settings and non-connecting of SNS accounts), others – equally non-engaging and not requiring specialized skills – are not taken at all or are rarely taken by more than half of the respondents (e.g. private mode in browser, use of different browsers, installing plug-ins against tracking or deleting cookies in the browser). This shows that privacy practices that can easily protect users from surveillance capitalism are not taken.

C. Hypothesis 1 testing. Users with extensive knowledge and a negative attitude towards surveillance capitalism undertake IPPP.

In order to check the relationship between the level of knowledge and attitude on surveillance capitalism (KASC), and the level of online institutional privacy protection practices (IPPP), a rho-Spearman correlation analysis was carried out. Table 4 below shows the correlation coefficients from the analysis.

Correlation analysis did not show any statistically significant relationship between the level of KASC and the level of IPPP: *rs = 0.10, ni*. This means that in the surveyed group, both people with high and low knowledge about surveillance capitalism apply similar practices in the scope of online privacy protection. The level of knowledge and the negative attitude do not affect the online privacy protection practices. Therefore, hypothesis 1 was not confirmed.

Table 4. Correlation and dependence between the level of knowledge and attitude on surveillance capitalism and the level of online privacy protection practices in the sample under review (*N = 177*)

	Knowledge and attitude on surveillance capitalism (KASC)	
	rho-Spearman	Significance level
Online privacy protection practices (OPPP)	0.10	0.193

D. Hypothesis 2 testing. Users participating in classes or workshops on internet safety and privacy (ISP) are much more likely to undertake online institutional privacy protection practices (IPPP)

In order to verify whether people participating in-school or out-of-school activities on ISP differed from those who did not participate in such classes, in terms of the level of IPPP, an analysis was carried out using Student's t-test for independent tests. Table 5 shows the results obtained in the study.

Table 5. Characteristics of the level of IPPP among participants (N=87) and non-participants (N=90) in classes/workshops on ISP in the network – student's t-medium difference

Variable	**Internet safety and privacy (ISP) classes or workshops attendance**	***n***	***M***	***SD***	***Min***	***Max***	Q_1	***Mdn***	Q_3	***t***	***p***
Online institutional privacy protection strategies (IPPP)	Yes	87	43.05	8.25	27	69	37.50	44	49	1.98	0.050
	No	90	40.32	10.02	20	62	32	42	48		

Remark : *n* – number; *M* – average; *SD* – standard deviation; *Min* – lowest value; *Max* – highest value; Q_1 -first quartile; *Mdn* – median; Q_3 – third quartile; *t* – student's t-test result for independent samples; *p* – significance level for the *t test*

The Student's t-test for independent samples showed statistically significant differences between the groups in the range of the analyzed variable: *t (170,72)=1.98; p <0.050; d=0.30* – this means that people participating in classes or workshops on ISP presented a higher level of IPPP than those who did not participate in such classes, so they used these practices more often.

Conclusions

The purpose of the study was to determine the knowledge and attitudes on surveillance capitalism of adolescents in Poland aged of 18–19, and with what frequency they undertake institutional privacy protection practices. The study showed that adolescents present diverse knowledge and attitudes on surveillance capitalism as well as a various levels of online protection practices. However, the majority presented moderate knowledge and a lack of a clear attitude (59.32%), and a large group of adolescents presented a moderate level of protection privacy practices (79.66%). Such a large number of moderate indications on both scales may result from the issue being too abstract, unrelated to their experience as Internet and mobile devices users. Also, the fact that the questions mostly concerned general issues and less frequently referred to specific social media, could also affect a large percentage of such responses.

The analyses did not show statistically significant relationships between the level of knowledge and attitudes of the respondents on surveillance capitalism and the level of their online institutional privacy practices. At this point, however, it should be noted that the majority of respondents (N=105) presented moderate knowledge and attitudes. The lack of a connection between knowledge and attitudes about surveillance capitalism and the practices of privacy protection may be explained by factors that influence the shaping of practices, as mentioned in the theoretical part. As the researchers point out, one of the most important factors affecting privacy practices is the negative experience of privacy violations (Trepte et al. 2014; Büchi, Just, Latzer 2016). In this study, this relationship was not analyzed; however, a large number of "never" and "seldom" responses to such practices as turning off geolocalization when not used, modification of default settings after installation, or verification of the author and source before uploading may indicate that the respondents do not see the risks associated with the violation of institutional privacy.

The analysis of the correlation between participation or non-participation in classes or workshops on internet safety and privacy (ISP), and the level of intensification of online institutional privacy protection practices (IPPP), has brought interesting results. Statistically significant differences in the level of the IPPP were observed only in relation to the group of respondents participating in classes/workshops on ISP. They concerned such practices as: verification of the source and author of the application before downloading, checking what kind of access on a mobile device is requested for the installed application, disabling geolocation on a mobile device or social networking site when not using the navigation or a map function, modifying the supplied privacy settings on a mobile device, or checking the permissions the new page requests when the respondents log in using a social media account. Interestingly, in the case of such strategies as installing plug-ins for search engines that protect against tracking and private data collectors, using a mailbox that encrypts data, deleting cookies or using various search engines to protect digital identity, a similar

level of intensification was observed in both groups. Perhaps the differences arise from the fact that certain privacy practices are more engaging and require more specialist knowledge (e.g. installing plug-ins in search engines against tracking and private data collectors or using a mailbox that encrypts data) and habitual repetition, which can be defined as habitual privacy protection strategies (e.g. deleting cookies or using various search engines).

Interpreting the differences described above on online institutional privacy practices, it is worth referring to the concept of the types of privacy expressed by Katie Raynes-Goldie (2010). It distinguishes social privacy – when a user wants to protect their personal data against the misuse by other users, and institutional privacy – when a user wants to protect themself against data collection by companies and institutions. Each of these types requires different practices (Matzner et al. 2016). Institutional privacy protection involves the use of more advanced tools, which requires greater technical competence related to, for example, changing the application settings or installing an appropriate program. It also requires more active practices that "serve to build a protected sphere" (Matzner et al. 2016, p. 282).

The result of the study can be used to develop activity programs devoted to online privacy in the context of surveillance capitalism. They also show that although the majority of respondents had moderate knowledge and attitudes about surveillance capitalism, which may result from insufficient knowledge of the subject matter, the participation in specialized activities/workshops can influence the level of intensification of online privacy protection strategies. However, the conclusions presented in the article contain some limitations. The study did not verify what kind of specific contents were implemented within the framework of the classes and workshops on internet safety and privacy (ISP) in which the respondents declared participation. A detailed analysis of the issues carried out during classes and workshops could additionally show how effective those educational impacts were and what factors influenced the respondents.

Acknowledgements

The author would like to thank anonymous reviewers for constructive comments. The particular thanks are also due to Onno Hansen-Staszynski for his critical remarks on the first version of the questionnaire and Aleksander Skrzypek for the proofreading of the text, as well as for all those who helped in reaching the respondents.

References

Acquisti A., Gross R. (2006). Awareness, information sharing, and privacy on the Facebook. https://dataprivacylab.org/dataprivacy/projects/facebook/facebook2.pdf, 23.03.2018.

Andrejevic M. (2012). *Exploitation in the data-mine*. In C. Fuchs, K. Boersma, A. Albrechtslund, M. Sandoval (Eds.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. Routledge: New York, pp. 71–88.

Andrejevic M. (2014). Big Data divide. *International Journal of Communication*, 8, pp. 1673–1689.

Barnes S. B. (2006). A privacy paradox: social networking in the United States, *First Monday. Journal on the Internet*, Vol. 11(9). http://firstmonday.org/issues/issue11_9/barnes/index.html, 03.02.2018.

Blank G., Bolsover G., Dubois E. (2014). New Privacy Paradox: Young people and privacy on social networks sites. Global Cyber Security Capacity Centre: Oxford. https://www.oxfordmartin.ox.ac.uk/downloads/A%20New%20Privacy%20Paradox%20April%202014.pdf, 12.12.2018.

boyd d. (2014). *It's complicated. The social lives of networked teens*. Yale University Press: New Haven, London.

boyd d., Crawford K. (2011). Six provocations for Big Data. Retrieved from http://softwarestudies.com/cultural_analytics/Six_Provocations_for_Big_Data.pdf, 12.12.2018.

boyd d., Hargittai E. (2010). Facebook privacy settings: who cares?, *First Monday. Journal on the Internet*, Vo. 15(8), http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589, 21.03.2018.

Büchi M., Just N., Latzer M. (2016). Caring is not enough: the importance of Internet skills for online privacy protection, *Information, Communication & Society, 20*(8), 1261–1278. Retrieved from https://doi.org/10.1080/1369118X.2016.1229001, 21.03.2018.

Citron D. K., Pasquale F. A. (2014). The Scored Society: Due Process for Automated Predictions, *Washington Law Review*, Vol. 89, p. 1–33.

Couldry, N., & Mejias, U. A. (2018). Data colonialism: Rethinking Big Data's Relation to the Contemporary Subject, *Television & New Media*.

Culver, H. S., & Grizzle, A. (2017). Survey on Privacy in Media and Information Literacy with Youth Perspectives. Paris, France: UNESCO. Retrived from http://unesdoc.unesco.org/images/0025/002589/258993e.pdf, 21.03.2018.

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*, Vol. 15(1), pp. 83–108.

Degli Esposti, S. (2014). What big data meets dataveillance: The hidden side of analytics. *Surveillance and Society*, Vol. 12 (2), pp. 209–225, www.surveillance-and-society.org, 07.04.2018.

Digital in 2018. (2018). We are social. Retrieved from https://digitalreport.wearesocial.com/

Dijck van J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, Vol. 12(2), pp. 197–208.

European Union, DG COMM. (2016). *Flash Eurobarometer 443. Raport e-Privacy*. European Union: Brussels, https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy, 07.01.2018.

Halavais A. (2009) *Search Engine Society*. Polity Press.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), article 7.

Jernigan C., Mistree F.T. B. (2009). Gaydar: Facebook frendships expose sexual orientation, *First Monday*, 14 (10)/ https://journals.uic.edu/ojs/index.php/fm/article/view/2611/2302.7, 21.03.2018.

Kennedy H., Poell T., Dijck van J. (2015). Data and agency, *Big Data & Society*. https://doi.org/10.1177/2053951715621569, 12.01.2019.

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

Kosinski M., Stillwell D., Graepel T., *Private traits and attributes are predictable from digital records of human behavior*, „Proceedings of the National Academy of Science" 2013, vol. 110, pp. 5802–5805.

Latour B. (2007). Beware, you imagination leaves digital traces, http://www.bruno-latour.fr/sites/default/files/P-129-THES-GB.pdf, 07.10.2017.

Litt E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior*, vol. 29, pp. 1649–1656.

Lutz C., Ranzini G. (2017). Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder. *Social Media + Society*. https://doi.org/10.1177/2056305117697735

Lyon D., Bauman Z. (2013). *Liquid surveillance. A conversation*. Cambridge: Polity Press: Cambridge.

Matzner T., Masur P. K., Ochs C., von Pape T. (2016). *Do-It-Yourself Data Protection – Empowerment or Burden?* In S. Gutwirth, R. Leenes, P. De Hert (Eds.), *Data Protection on the Move*. Law, Governance and Technology Series 24. Springer: Dordrecht, pp. 277–305.

Mayer-Schonberger V., Cukier K. (2013). *Big Data: A Revolution that Will Transform how We Live, Work, and Think*. Boston, New York: An Eamon Dolan Book/ Houghton Mifflin Harcourt.

Milanesi C. (2018). *US Consumers Want More Transparency from Facebook*; https://techpinions.com/us-consumers-want-more-transparency-from-facebook/52653, 21.03.2018.

Newman N, Fletcher R., Kalogeropoulos A., Levy D. A. L., Nielsen R. K. (2017). *Reuters Institute Digital News Report 2017*. Oxford, Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf, 21.03.2018.

Nadler A., Crain M., Donovan J. (2018). *Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech*. Data&Society Research Institute; https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf, 21.03.2018.

Nissenbaum H. (2011). A contextual approach to privacy online. *Daedalus*, Vol. 140 (4), pp. 32–48, https://ssrn.com/abstract=2567042, 04.03.2018.

Nissenbaum H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books: Palo Alto, CA.

Raynes-Goldie K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook, *First Monday*, Vol. 15 (1–4), http://dx.doi.org/10.5210/fm.v15i1.2775, 04.04.2018.

Sundar S. S., Marathe S. S. (2010). Personalization versus Customization: The Importance of Agency, Privacy, and Power Usage, *Human Communication Research,* vol. 36(3), pp. 298–322.

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*, Vol. 19(2), pp. 248–273.

Tamir D.I., Mitchell J.P. (2012). Disclosing information about the self is intrinsically rewarding, *Proceedings of the National Academy of Sciences*, vol. 109 (21), pp. 8038–8043.

Trepte S., Dienlin T., Reinecke L. (2014). *Risky behaviors: How online experiences influence privacy behaviors,* In *Von der Gutenberg-Galaxis zur Google-Galaxis*, B. Stark, O. Quiring, N. Jackob (Eds.). UVK, pp. 225–244.

Trepte S., Teutsch D., Masur P. K., Eicher C., Fischer M., Hennhöfer A., Lind F. (2015). *Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS),* In *Reforming European Data Protection Law*, S. Gutwirth, R. Leenes, P. de Hert (Eds.). Dordrecht: Springer Science+Business Media, pp. 333–365.

Turow J., Feldman L., Meltzer K. (2005). *Open to Exploitation: America's Shoppers Onlineand Offline. A Report from the Annenberg Public Policy Center of the University of Pennsylvania*; http://repository.upenn.edu/asc_papers/35, 21.03.2018.

Uricchio W., *The Algorithmic Turn: Photosynth, Augmented Reality and the Changing Implication of the Image*, „Visual Studies" 2011, vol. 26(1), p. 27.

Young A. L., Quan-Haase A. (2013). Privacy Protection Strategies on Facebook, *Information, Communication & Society,* vol. 16 (4), pp. 479–500.

Zuboff S. (2019). *The Age of Surveillance Capitalism: The Fight for the Future anf New Frontier of Power*. London: Profile Books.

Zuboff S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, Vol. 30, pp. 75–89.