
Individual Online Privacy Management among Polish Internet Users – Outline of Issues and Research Review

Malwina Popiołek¹ and Maciej Czaplewski^{2,*}

¹*Jagiellonian University in Kraków, Poland*

²*University of Szczecin, Poland*

**Corresponding Author: maciej.czaplewski@wzieu.pl*

Received 3 July 2017;
Accepted 5 August 2017

Abstract

The paper describes an outline of selected issues connected with online privacy management in Poland. It deals with the problem of theoretical contexts of the subject and presents the concept of Individual Online Privacy Management. It also shows the legal status concerning privacy regulations in Poland. The article also provides a brief overview of research, concerning how Polish society respond to changes in law, which are related to online privacy.

Keywords: Internet Privacy, Individual Privacy Management, cyber security, privacy protection, personal data protection.

1 Introduction

One of the main issues associated with online safety is the matter of Internet users privacy protection. This subject appears recently quite often. The issue of cyber-security and the protection of private data of individuals can be considered from two perspectives. Firstly, in the context of formal and legal regulations ensuring the safety of people using various types of e-services. Secondly, in the context of active concern for privacy by the users themselves.

Journal of NBICT, Vol. 1, 33–44.

doi: 10.13052/nbjict1902-097X.2017.003

© 2017 River Publishers. All rights reserved.

As for the legal regulations providing Internet users protection of their data, we can say, that in the face of intense changes in the area of information and communication, it turns out that the current regulations do not protect users as much as necessary, and new ones are often introduced with a great delay. The legal protection of privacy is therefore still a huge challenge for international institutions introducing law and regulations, and the universality of using the Internet or mobile phones is constantly increasing the number of threats to the security of personal data [Krzysztofek 2012].

As noted by J. Wiczorkowski ease of communication and data processing, much more than previously, increases the risk of privacy violations as well as units surveillance. The problem is due to the new technical possibilities that enabled on a massive scale a real time data processing of individuals. This allows not only to obtain information, but also to track Internet users. In such situation there is a risk of privacy violations on an unprecedented scale. Processing of personal data may be associated with different needs realized in particular by private individuals, businesses or public administration [Wiczorkowski 2016].

It seems, therefore, that to increase the online security one should consciously take care of it, to safely communicate private information. However, to protect privacy in an active way, it is necessary to have appropriate digital competencies. Lack of such competences exposes people who use e-services to numerous threats, even including digital exclusion [Budzewicz-Guzlecka, 2010, p. 241]. However, taking into account the subject of this article we need to say that insufficient attention to network privacy may result in exposure to cybercrime, and the risk that other, unauthorized parties will come into the possession of sensitive information about us.

In this article, the authors touch selected issues concerning the protection of online privacy. The article has a character of a review. It consists of two fundamental parts. The first one describes the concept of Individual Online Privacy Management. The second part presents and discusses research on the manner in which Internet users in Poland perceive various issues relating to online privacy, as well as their way of privacy management.

2 Theoretical Background

Privacy is defined differently. It is functioning in different contexts and on the ground of different scientific disciplines. Steven T. Margulis notes that in general there are three main groups of privacy definition: legal, common and empirical [1977]. Privacy can be understood for example as a protection of

one's personal space and the right to be let alone [Warren, Brandeis 1890]; as a right of the individual to withdraw from society and from social practices [Altman 1977], as well as one of the most important aspects of civil liberties and human dignity in general [Schoeman 1992].

The article deals with Individual Online Privacy Management. This concept corresponds with the approach of other authors, including A. Westin, H. Nissenbaum or W. Jones. According to A. Westin privacy is the claim of individuals to determine for themselves when, how, and, in particular, to what extent information about them is communicated to others [1967]. This Author treats privacy as a specific type of information – about a particular person – by putting this kind of information in the context of communication between individuals.

Individual Privacy Management is also a reference to the term created and popularized by William Jones as the concept of Personal Information Management (PIM). However, Jones did not write about privacy, but about information management. The PIM concept introduced by him refers to any human actions performed in order to acquire, organize, maintain and use of relevant information for individuals [Jones 2008]. Emphasized is here the active side of information management. So if we restrict the type of information to private information concerning only the specific person managing them, we will deal with the management of private information, which can be otherwise determined precisely as managing privacy – and therefore an active concern for the communication of private information.

H. Nissenbaum writes about managing privacy in a fairly broader sense. This author also strongly identifies the privacy with communication of private information and she argues about personal information flow, but she believes it requires to take a wider context into account. In her view, control of private information is always embedded in a specific social context – what information, to whom, when and in what kind of situation can be transmitted [Nissenbaum 2010].

According to this, authors of this article formulated the concept of Individual Online Privacy Management, understood as information management, but only a private one (related directly to a specific person and concerning only this particular person). By this, it should be understood, as all consciously actions undertaken by individuals aimed at current control over private information and in particular aimed at the fact that this information could not be used by other persons or third parties. At the same time it seems important to take into account the individual character of such management, because managing privacy should not be limited only to active actions taken by an

individual. Often, not the users themselves, but online service providers are those, who manage privacy for the users (so called passive and active privacy management) [Yao 2011].

3 Privacy in Polish Law

The issue of privacy protection is also important from the legal point of view. As noted by M. Pryciak: In the Polish legal system privacy protection closely corresponds with the system of information protection and personal data protection (including medical data), which are being collected and processed by various institutions [Pryciak, p. 224]. At the moment, threats to privacy concern primarily the functioning of modern information systems, which actions are based on electronic data processing techniques. Capabilities of these systems are on a steady rise (e.g. e-commerce systems [Drab-Kurowska 2013, p. 502]), resulting in the possibility of gathering a vast amount of information about the object, its habits and preferences. Possession and use of these data increases risks of breaching privacy, and their proper protection, not only legally, should be a priority in this area of state actions.

In Poland, protection of privacy is guaranteed, among others, by The Constitution, and in the context of ICT especially two articles: article 49, which says that: “The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute”; and article 51, paragraph 1 which states: “No one may be obliged, except on the basis of statute, to disclose information concerning his person” [Polish Constitution, 1997].

At this point one should also mention the upcoming General Data Protection Regulation (GDPR). For more than 20 years, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data has been in force.

Over time, this directive has become less adequate to the modern state of Internet development. In order to improve the effectiveness of data protection across the EU, the GDPR regulation was introduced. It entered into force on the 17th of May 2016 and its regulations will be mandatory throughout the EU from the 25th of May 2018. The main changes are:

- the clarification of the personal data concept,
- regulation in the field of privacy by design and privacy by default,
- right to erasure,

- profiling limitation,
- one-stop shop mechanism,
- the obligation to designate a Data Protection Officer [EU, 2016].

Basing on information that can be found on the pages of the Polish Ministry of Digital Affairs [2017], actions and consultation on the implementation of the requirements presented by the GDPR are in progress. However at this moment there are no other, specific information regarding this issue available.

According to Bartosz Dylağ [2017] in general, the biggest problem seems to be the time, that is needed to adjust everything within a year. This may affect mainly local governments, because if they do not make it on time, they will be fined. And most probably they will fail, because they do not have enough financial means to make all the changes.

Moreover, arousing emotions in Poland in 2016 an amendment to the law concerning the activities of various state services, including police, special services and fiscal control authorities was introduced. This law is sometimes referred as a surveillance act, because it significantly increases the power of services in the field of data collection. Hitherto, police and other services could obtain information on the needs of their proceedings only after submitting an official letter to the Internet Service Providers. Now, this access is facilitated by specially prepared for this purpose Internet connections. Therefore no longer a contact with ISP is necessary [Feliksiak, CBOS report, 2016].

4 Attitudes to Privacy Protection

Studies on the privacy management practices are carried out systematically by researchers representing various disciplines as well as by institutions monitoring social life. In the literature we can find examples of interesting analyzes with the aim to diagnose attitudes towards privacy. One of the most interesting is the research of attitudes towards privacy conducted by A. Westin, and later verified by other researchers. This author, basing on the analysis of empirical research conducted in the USA in the environment of the traditional consumers market, identified three types of attitudes towards the privacy protection [1996]:

- pragmatic attitude – characterized by the fact that the person providing private information assesses the potential gains and losses associated with this. Such attitude was demonstrated by the majority of Westins respondents (over 50%);

- fundamentalist attitude – characterized by the fact that a person protects its privacy, giving up even the potential benefits (such an attitude presented about 25% of the respondents);
- carefree attitude – characterized by a low level of concern for privacy (25% of respondents).

Later studies by other authors (see. Sheehan 2002) delivered results with slightly different proportions. It showed, however, another interesting and important issue. It turned out that many of those who pragmatically approached the protection of personal data did not have the awareness to what extent and how the data are being processed and used. Familiarization with this information caused mostly a change from the pragmatic attitude to the fundamental one [after: Kołodziejczyk, pp. 26–28].

5 Individual Online Privacy Management among Polish Internet Users

In Poland, research on the individual privacy management among Internet users are conducted by large research centers (like CBOS – Public Opinion Research Centre, which is co-financed from the state budget) as well as by individual researchers.

According to the representative survey (conducted by CBOS), Poles eagerly use online services (especially those offered by social networking sites) and do not feel any particular privacy risk threats. Most popular and most widely shared data are e-mails (63%), date of birth (56%) and photos with own image (52%). A large part of the Polish Internet users also share data about their location (37%), place of residence (35%), marital status, hobbies and political views, as well as gives their phone numbers (over 30% in each case) [CBOS 2015]. An important variable regarding data sharing is the age of the respondents. It is easy to notice that the younger the Internet users the more often and willingly they provide private information on-line. The CBOS distinguished 3 age groups: 18–24 (this group most willingly shared private information online and did it among almost everyone – not only their friends or specific institutions); 25–34 (in this group preferences in the provision of private data were similar); and 35–64 years (a group most conservative in terms of data sharing – if they already provide information then it is generally to a specific audience) [Feliksiak, CBOS report 2015].

In terms of new law regulations the views of Poles are quite diverse. Generally, one can notice a trend that the younger Internet users, the more

doubts regarding the increase of the rights to obtain personal information by the state. Almost half of Poles also believes that the state services should have access to personal data of Internet users for the purpose of crime prevention [Feliński, CBOS report 2015]. At the same time in the same study we can find that 54% of Poles have not heard about the amendment to the rules on data collection and 27% came into contact with information on this subject, but does not know the nature of these changes. Only 19% of those surveyed by CBOS possessed some knowledge within this area [CBOS 2016].

Research on the privacy management among Polish Internet users are also carried out by individual authors like Ł. Kołodziejczyk [2014] or J. Wiczorkowski. Kołodziejczyk was investigating privacy in the context of the social media use. The author conducted qualitative research (in-depth interview) in the group of young learners (and thus in a group with a statistically high level of e-competences), which actively used social media. It is a complicated multi-level analysis showing many aspects that are often hidden in quantitative research.

Students surveyed by Kołodziejczyk pointed out that, in their opinion, the privacy management in the internet is not an easy thing to do. On one hand because they feel the need to share private information (the way of functioning of social networking sites such as Facebook promotes communication of private information). On the other hand, they are aware that the more sensitive data they provide, the more difficult it is to keep principles of security [Kołodziejczyk pp. 130–131]. Interestingly, the surveyed students noticed two contexts of privacy threats: the institutional and the social. The first referred to the use of their private content by unauthorized entities (eg. for marketing purposes by companies), while the second context concerned the social relations – mainly sharing private information with friends during the use of social networking sites. In the first case people had a good sense of insecurity, while in the second, a rather small one [Ibid].

What is also interesting, the research shows that users of social network sites know that they can protect their privacy better eg. through appropriate privacy settings. But not everyone is able to do it. Respondents declared that the amount of time needed to search for the desired privacy settings is often disproportionate to the expected benefits from it, and they are also discouraged by the fact that even the desired settings do not guarantee complete security [Kołodziejczyk, p. 131]. Difficulties in finding appropriate privacy settings may be also due to the fact that the concern for users' privacy from the side of the owners of sites such as Facebook is often only apparent. Despite the declarations of such companies that the way of handling the interface is simple

and user-friendly, it is hard to resist the impression that in the case of privacy settings many of them are deliberately hidden away.

Research on the online privacy management is also conducted by J. Wiczorkowski [2016]. This author carried out a survey on a non-representative sample of 256 students. The aim of this study was to determine the situations in which the subjects agree on a breach of their online privacy. The research shows that the subjective assessment of acceptance of privacy violations for different purposes is highly diversified. The students showed a fairly high tolerance for situations where their privacy was violated for the purposes of public security e.g. in order to fight or prevent crime. Completely opposite attitude was shown when it came to the use of private data for commercial purposes. Respondents were therefore willing to agree to a privacy violation if it would serve legitimate, in their opinion, purposes, and expressed objections especially in the case of individualized advertising content (online advertising displayed in connection with the activity of a particular user, detected of his location, etc.) [Wiczorkowski 2016].

6 Discussion and Conclusions

According to the survey, Poles eagerly share private information, while at the same time are quite poorly aware of the issues related to online privacy management. More than half of Poles had not heard about changes in the law regarding private data availability. One quarter of the respondents have heard about it, but do not know how the details look. [Feliksiak, CBOS report 2016]. This demonstrates the need to deepen research in this area to find out if the willingness to publish private information online is caused by the actual sense of security, or rather by the lack of sufficient knowledge about the potential risks associated with the loss of privacy. This is especially important in the context of data mentioned above, when researchers find out that the knowledge about actual use of data can change the approach to online privacy managing radically.

The number of researches conducted in Poland on privacy is still insufficient. There is a lack of both quantitative analysis covering the entire population and qualitative research. The results obtained so far are quite ambiguous, and therefore it is necessary to conduct further research in this area. Especially desirable are studies showing individual privacy management from the generational perspective since significant differences in the approach to the management of online privacy between younger and older people are

quite obvious and easy to see. However, differences in online behavior are reflected also by other social divisions [see. Kuczera, 2012].

Another issue is the great diversity and multidimensional nature of the problem of individual online privacy management. On the basis of presented results we can see that in privacy studies it is necessary to take into account the context of communication, which was mentioned by Nissenbaum. This requires carrying out a multi-level research among groups of different socio-demographic structure. Only then it will be possible to obtain a more precise data on how to manage online privacy.

Reference

- [1] Altman I. (1977). Privacy regulation: culturally universal or culturally specific? *J. Soc. Issues* 33, 66–84.
- [2] Budziewicz-Guźlecka, A. (2010). Istota wykluczenia społecznego w społeczeństwie informacyjnym (The essence of social exclusion in the Information Society), *Informatyka ekonomiczna*, in *Zeszyty Naukowe Uniwersytetu Ekonomicznego*, eds Nowicki, H. Sroka and I. Chomiak-Orsa (Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego), 241–249.
- [3] Constitution of the Republic of Poland (1997). *Constitution of the Republic of Poland*. Dziennik Ustaw No. 78, item 483;
- [4] Drab-Kurowska A. (2013). Polityka konkurencji na rynku e-commerce (Competition Policy on e-commerce market). *Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług* 1, 501–511.
- [5] Directive 95/46/EC (2017). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Available at: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf [accessed 27 July, 2017].
- [6] Dyląg, B. (2017). *RODO: Samorzady Narazone na Drakońskie Kary*. Available at: <http://www.portalsamorzadowy.pl/spoleczenstwo-informacyjne/rodo-samorzady-narazone-na-drakonskie-kary,91247.html> [accessd July 28, 2017].
- [7] Feliksiak, M. (2016). *Inwigilacja w Internecie (Surveillance on the Internet)*. CBOS Report. Available at: http://www.cbos.pl/SPISKOM.POL/2016/K_072_16.PDF [accessed October 12, 2016].

- [8] Feliksiak, M. (2015). *Bezpieczeństwo w Internecie (Safety on the Internet)*, CBOS Report. Available at: http://cbos.pl/SPISKOM.POL/2015/K_109_15.PDF [accessed October 12, 2016].
- [9] Jones, W. (2008). *Keeping Found Things Found*. New York, NY: Morgan Kaufmann Publishers.
- [10] Kołodziejczyk, Ł. (2014). *Prywatność w Internecie (Privacy on the Internet)*. Warszawa: Wydawnictwo SPB.
- [11] Kuczera, K. (2012). *Postawy Jako Bariera Rozwoju Społeczeństwa Informacyjnego w Polsce (Attitudes as an Obstacle to Development of the Information Society in Poland)*, Szczecin: Zeszyty Naukowe Uniwersytetu Szczecińskiego.
- [12] Krzysztofek, M. (2012). Prawo do bycia zapomnianym “i inne aspekty prywatności w epoce Internetu w prawie UE (The right to be forgotten” and other aspects of privacy in the Internet Age in the EU law). *Europ. Prz. Sądowy* 8, 29–34.
- [13] Margulis, S.T. (1977). Conceptions of privacy: current status and next steps. *J. Soc. Issues*. 33, 5–21.
- [14] Nissenbaum, H., (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press.
- [15] Polish Ministry of Digital Affairs (2017). Available at: <https://mc.gov.pl> [accessed July 26, 2017].
- [16] Pryciak, M. (2010), Prawo do prywatności (The right to privacy). *Stud. Erasm. Wratislaviens.* 4, 211–229.
- [17] EU 2016/679 (2016). *Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf [accessed July 28, 2017].
- [18] Schoeman, F. (1992). *Privacy and Social Freedom*. Cambridge: Cambridge University Press.
- [19] Sheehan, K. B. (2002). Toward a typology of internet users and online privacy concerns. *Inform. Soc.* 18, 21–32.
- [20] Warren, S., and Brandeis, L. (1890). The right to privacy. *Harvard Law Rev.* 4:5.
- [21] Westin A. (1967). *Privacy and Freedom*. New York, NY: Atheneum.

- [22] Westin A. (1996). *Privacy in the Workplace: How Well Does American Law Reflect American Values?* Available at: <http://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=4039&context=cklawreview>
- [23] Yao, M. Z. (2011). "Self-protection of online privacy: a behavioral approach," in *Privacy Online Perspectives on Privacy and Self-Disclosure in the Social Web*, eds S. Trepte, and L. Reinecke, (New York, NY: Springer), 111–125.
- [24] Wiczorkowski, J. (2016). Ochrona Prywatności w Erze Big Data, (Protection of Privacy in the Era of Big Data), *Nierówności społeczne a wzrost gospodarczy*. [in print].

Biographies



Malwina Popiołek – completed her Ph.D. dissertation in social science at Opole University. Since 2016 she is a member of the Faculty of Management and Social Communication at Jagiellonian University in Cracow. She lectures also at Opole University. Her research and teaching focuses especially on new media and ICT. She is also interested in digitalization, e-government, privacy and social media management. E-mail address: m.popiolek@uj.edu.pl



Maciej Czaplewski received his Ph.D. and M.Sc. degrees in Economy at the University of Szczecin. He attended also Malärdalen University Västerås, Sweden where he received his B.Sc. Since 2003 he works at the Faculty

of Management and Economics of Services on the University of Szczecin. His research focuses on the use of modern ICT in economy with a special regard towards electronic commerce. He became “insurance specialist in UE” (Geprüfter Versicherungsfachwirt) after passing required exam accredited by IHK (Industrie- und Handelskammer) in Germany.