Chapter 6

Generation Y and Internet Privacy: Implication for Commercialization of Social Networking Services

Zdenek Smutny
University of Economics, Czech Republic

Vaclav Janoscik
Academy of Fine Arts in Prague, Czech Republic

Radim Cermak
University of Economics, Czech Republic

ABSTRACT

This chapter addresses the issue of privacy settings with a focus on Generation Y from a technological, social, generational, cultural and philosophical point of view. After introducing the issue of Internet privacy and other relevant areas—generational and cultural differences, the philosophical framework, the postinternet condition, the possibilities of processing and (mis)using personal data, and privacy policy—the authors present their perspective on the issue, drawing implications for individuals and organizations based on their own research and other relevant studies. The authors discuss the possible implications in terms of a prospective use of personal data by companies (e.g., for marketing and management) and possibility of processing user data. Such perspective will allow them to formulate a critical basis for further assessment of social networking and Generation Y’s attitudes to privacy. The chapter concludes by outlining several recommendations concerning the commercialization of social networking services with respect to the constantly changing conception of privacy.
INTRODUCTION

This chapter provides an interdisciplinary perspective on the attitude of today’s young people from Generation Y towards self-disclosure and on the impact of such behaviour on the individual, as well as on the challenges for commercial exploitation of social networking services. A definition of Generation Y is given in the part Cultural and generational differences. From a firm’s perspective, there are two reasons why it is important to focus on Generation Y:

- Generation Y has a positive attitude to information and communication technologies (ICT) (Valentine & Powers, 2013), which are already a common element in their lives (Benckendorff, Moscardo & Pendergast, 2010, p. 20; Lahtinen, 2012). This part of their life is reflected in social networking services and thus shared with other people. These (personal) data from various Internet-based services can be used in commercial and professional activity.
- Members of Generation Y are economically active. From a firm’s perspective, this means that they can act as customers or as employees.

Internet privacy is viewed as the right of a subject (human) for the protection of their personal data and the way they are handled (Puddephatt et al., 2012) – i.e. stored, processed, used (including changes in their use), provided to third parties and displayed on the Internet. The information collected during an individual’s interaction in a particular social networking service can be divided into personally identifying information (e.g. information that relates to a particular person or identifies them) and non-personally identifying information (e.g. anonymous information about an individual’s behaviour on a web portal). (Cermak, Smutny & Janoscik, 2014)

A long-term trend in companies’ activity is the collection of such data and its subsequent evaluation for various purposes of the companies (e.g. marketing). The sources of these data are the information and front-end systems of an organization (e.g. the collection of consumer data) (Roberts & Zahay, 2012, pp. 101-105), as well as freely accessible data on the Internet (e.g. the discussion of people on a particular web) (Sperkova & Skola, 2015). This also affects common users, who interact within various Internet-based services and thus create a large amount of personal data – this concerns mainly social networking services. The reason for such behaviour is today’s information society, which unobtrusively prompts users to share their personal information on the Internet (e.g. people are positively motivated to share their personal information). This can also be described by the term self-disclosure (Benson, Saridakis & Tennakoon, 2015). Personal information accessible on the Internet can thus, on the one hand, help companies and their customers, from whom they can receive feedback or achieve personalisation to their customers based on individual data processing. On the other hand, it is a temptation for third parties to exploit these data.

A dual perspective (individual and firm) will be considered in this chapter. Companies should be aware of the challenges connected with individuals’ Internet privacy, because those individuals may comprise customers and also their employees. Their personal information could be used for bullying or manipulating them to reveal a company secret or to become a serious security risk (Benson et al., 2015). This chapter focuses on the use of individual information disclosed on social networking services, primarily for marketing and management. Such systemic view on Internet privacy may be beneficial for organizations.
This chapter is organized as follows: Firstly, it introduces the theoretical foundations of technological, social, generational, cultural and philosophical issues of Internet privacy. It then discusses Generation Y’s approach to self-disclosure on social networking services of users from France and the Czech Republic. The final two sections suggest future directions of research and highlight implications for policy and practice. This means particularly the possibilities of commercialization of available personal data.

BACKGROUND

In this section authors address various issues of privacy in the social web. After stressing the cultural and generational differences, the authors raise some questions stemming from the work of various thinkers in order to frame the problem of privacy in the postinternet condition. Postinternet is described as the ‘moment in which the Internet is no longer a fascination or taboo, but rather a banal fact of daily living’ (Arche, 2013). The postinternet condition is typical for the daily lives of Generation Y. The aim of the thematic sections is to expose essential standpoint in respect to Internet privacy connected with the needs of firms and other commercial activities online.

Cultural and Generational Differences

This chapter is focused on the representatives of the so-called Generation Y. The term Generation Y is nowadays assigned to young people who are newly economically active or will become economically active in the near future. Another important aspect is that this is the first generation that could in their childhood use ICT, especially computers and mobile devices. Its specificity can be defined using the time chronology.

Each generation overlaps, but we can, nevertheless, introduce at least an approximate chronological division: Baby Boomers (from the mid-1940s up to the early 1960s), Generation X (from the early 1960s to the early 1980s), Generation Y (from the early 1980s to the early 2000s), Generation Z (from the mid-1990s up to the early 2010s), Generation Alpha (after 2010). Representatives of Generation Y are the descendants of a significant generation called the baby boomers, who were born in the post-war period, and the oldest representatives of Generation X (Savage, 2011). Generation Y is also called the Next Generation, Millennials or the Net Generation and it is divided into three generation sub-units (Pendergast, 2010): Generation Why (born 1982-1985), Millennials (born 1985-1999) and iGeneration (born in 1999 -2002). In this chapter we focus on the first two sub-units. The reason for the focus on a selected group is the already mentioned fact that its members are gradually becoming fully economically active and are able to intuitively use modern Internet-based technologies (Benckendorff, Moscardo & Pendergast, 2010, p. 20; Valentine, Powers, 2013).

Along with the differences in generations, cultural differences should also be taken into account when discussing the differences in the approach to privacy. The term glocalization has been frequently discussed since the 1980s. It refers to the localization of a global product or service to a particular country or region. Web services are inherently ideal for global action and thus the issue of website localization for different cultures began to be researched intensively at the beginning of the millennium. The society of each country has its national traits, qualities, recognized values, habits, history and so on. All of this together creates a complex mix that forms the culture. It is therefore a complex concept that must be grasped somehow.
In this context, Hofstede’s cultural dimensions are the most widely used tool. We can describe culture of each state by these dimensions. There are many studies showing a higher efficiency of culturally localized websites or Internet-based services – e.g. (Vyncke & Bergman, 2010; Cermak, 2015). This fact suggests that people from different countries have different expectations and behaviour, even when it concerns so global a medium as the Internet. For instance Li et al. (2009) supports this influence of cultural values on the approach to the use of ICT with a focus on online services. The results show that time orientation plays a significant role in the willingness to use new technology. Long-term oriented cultures are more compliant to use new technologies, because the features of long-term oriented users fit the nature of technology use. An important problem presents the dimension of individualism/collectivism. Users with higher values of individualism are more confident when working with technology in general and would find it less difficult.

Culture (as well as age, as mentioned above) is an important factor also in terms of the approach to the use of personal data. Miltgen and Peyrat-Guillard (2014), for example, provide interesting results within Europe. There is a difference in the north and the south of Europe concerning the importance of responsibility as opposed to trust. Another difference regards disclosure as a choice in Southern and as forced in Eastern Europe. Concerning the age, more positive attitudes toward data management, greater responsibility and greater confidence in the ability to prevent possible misuse of data can be found within the Generation Y.

Moreover, culture is stated as an important factor in a field of privacy also in the today’s reflection about privacy in the information age (Dinev, 2014). The importance of culture show also previous articles of the author. Dinev et al. (2006) refer to the connection of cultural dimensions (especially Individualism-collectivism and Uncertainty Avoidance) and the concepts of trust and Internet privacy concerns and perceived risk, as the main variables for the use of services requiring personal data. Dinev et al. (2009) examined cross-cultural differences between South Korea and the United States in user behaviour towards protective information technologies and found that cultural factors are significant within the context of user attitudes and behaviour towards this type of technologies.

PHILOSOPHICAL ANCHORING OF SUBJECT PRIVACY

It is necessary not to lose sight of the theoretical and indeed the philosophical level. The reason is obvious: proceeding with the research of the issues concerning company growth or marketing would lead to a complete abandonment of the ethical or, more precisely, the normative and critical level, as illustrated by the relationship of ethical and economic behaviour of companies in (Sigmund, 2015). It is not possible only to propose how to target people within marketing; it is necessary to know what for and what social relations it affects or creates. It is impossible to simply describe what is being shared or kept in secret; it is necessary to know what concept of privacy it articulates. This attitude can prevent us from simply adhering to instrumental concepts of social media and privacy, for instance. More than ever before, it is important to realize that media, namely online social networks, are not mere means for our readymade identities and goals but that they involve their intrinsic rules of conduct deeply affecting our notions of identity, privacy or marketing communication. Therefore, the conclusion of this chapter is not simply deduced from research or the collected data itself, it rather springs from a deeper interest that is fuelled by critical thinking and philosophy.
These are inherently linked to art and its social imagination. Let us therefore begin with one artistic example – *Balconism* by Constant Dullaart (2014). It presents a text that is a kind of postinternet manifesto but also a gallery installation. On a general level, the balcony presents us with a spatial metaphor of the Internet itself. The basic, underlying condition of any conduct we take online is, that we are both in private and public. As on the balcony, we consider the space to be part of our private sphere. We exercise quite personal type of conduct here and that is why we actually talk about Internet privacy. But, on the other hand, we are visible. It does not matter whether someone actually watches us or uses our personal data; the important thing is that, potentially, we are being watched all the time, as if we were on a balcony. This brings us to the basic assumption concerning Internet privacy and its impact on our idea of the private sphere. Due to its inextricable connection with the public, we need on the one hand, to reflect its danger of abusing our private data (publically available), but on the other hand, we may address its mediatory potential, whether it is in political (the impact of social media in the Arab spring, for instance) or economic terms (tubers and bloggers).

On a theoretical level, we can summarize the historical development with Hannah Arendt’s influential book *Human Condition (Vita Activa)* (Arendt, 1998). She argues that (1) in the ancient polis, the private sphere of a household (*oikos*) was strictly disengaged from and subordinate to the public sphere of the agora; everybody (except for slaves and women, of course) was equal within the public sphere, no matter what their private interests were. Nonetheless, this hierarchy is overturned in (2) the modern times, with individuals being determined by their profession, class or social position – i.e. by their private realm, which invades the public sphere. We seem to be entering yet another stage (3), in which it is increasingly difficult to disentangle these two spheres. Our privacy is constantly redefined and used within the public realm (of the Internet). Let us now connect this brief remark to our issue. Unlike common inquiries into the problem of Internet privacy, we tend not to take the very concept of privacy as predetermined, unequivocal or universal; it simply cannot be identified as a set of personal data (e.g. email address, pictures, consumption preference). Contrary to such implicit preconceptions, we believe that privacy is a deeply multifactorial and flexible concept that is being redefined along with its cultural, historical and even technological context.

As such, it cannot be separated from other underlying philosophical conditions, such as social order, economic system or media channelling. It is precisely (but of course not exclusively) through the notion of privacy that the phenomena of the Internet and social networking in particular transform our social communication and culture. And from the opposite direction, Internet environment not only poses new challenges for our privacy and its protection (Young & Quan-Haase, 2013), but our very notion of privacy is fundamentally transformed in an entirely new perspective. In a sense, the hypermedia reality is brought to its pinnacle. This means that the Internet environment as a medium absorbs all other media that are directed towards plurality and heterotopia of content and forms, thus creating a new logic of transparency of media content (Bolter & Grusin, 1999), along with setting a new dynamic of accessing one’s private domain. Let us set the problem of privacy within a philosophical context with respect to its practices and human activities on three critical levels; namely in the context of (1) consumption, (2) freedom and (3) power.
Consumption

One of these lines is a critique of consumer culture. Perhaps the most radical formulation is provided by the so-called Frankfurt School and specifically Theodor Adorno. In his book *Minima Moralia* he states in the fragment *Asylum for the Homeless*: ‘The predicament of private life today is shown by its arena. Dwelling, in proper sense, is now impossible. (...) It is part of morality not to be at home in one’s home.’ (Adorno, 2005, pp. 38-39) Throughout the entire book Adorno aims at an analysis of alienation, particularly in terms of consumerist culture. He concludes that, due to mass reproduction penetrating into all spheres of life, even our privacy is not the domain of individual freedom.

In 1951, when the book was first released, he provided an insight into the prospective development of reproductive technologies and their impact on privacy. Adorno is preoccupied mainly with radio and television. Nonetheless, it points again to the lack of division between private and public. For Adorno, it stems from the false identity of individual and general implied by modern media, including the Internet. Our identity and privacy falls prey to the public sphere ruled by uniformity and commercial exploitation. Uniformity of the private sphere is thus enforced as a means of identification with the community. Privacy in terms of mass media and especially social networking is not a sphere that would be only opposed to the threat of misuse, and thus driven by the dynamics of protection against the logic of the media. It also works in reverse dynamic through the pressure to publish the private content by the user himself. As users, we are motivated by a desire to identify ourselves with others on the basis of common or uniform private contents (holiday or celebration pictures, as well as information about school or hobbies).

Freedom and Its Media Logic

While on the first level we addressed the uniformity enforced within the medium, in the next stage we need to address the problem of new possibilities which the media provide us with. For it is true that new means create new forms of communication and action. In this respect we may turn to Michel de Certeau, who provides us with critique of these possibilities of media as they do not enlarge our freedom but on the contrary they entangle our action within their own logic. Media strive for a deeper penetration of their mechanisms into our lives and specifically our privacy.

In the words of De Certeau, as he writes in the chapter ‘Reading as Poaching’ in his book *The Practice of Everyday Life*: ‘In any event, reader’s increased autonomy does not protect him, for the media extend power over his imagination, that is, everything he lets emerge from himself into the nets of the text – his fears, his dreams, his fantasized and lacking authorities. This is what the powers work on that make out of “facts” and “figures” a rhetoric whose target is precisely this surrendered intimacy.’ (De Certeau, 1984, p. 176) Though the text of 1980 was directed towards the medium of text and reading, we see its topicality in the perspective of social networking services. De Certeau shows here that the new options, such as the possibility to dispose of one’s own personal data, may not be an increase of privacy protection. Because our will to limit this access to our personal data is based on the idea (‘imagination’) we have about our privacy, which is already incorporated in the logic of the social networking services. In addition, this phantasm of ‘surrendered intimacy’ allures through the promise of authentic human presence within otherwise highly impersonal communication in the Internet environment. Nonetheless, we can be cautious or even ironical; we can play along the lines of the medium and still keep our position safe. In one word, we can poach. This also resonates in the Balconism of Constant Dullaart who calls for self-awareness, coding and encryption that spring from the very nature of the (Internet) environment we entered.
Power

Both the preceding levels of critique of media direct our attention to the issues of power, surveillance or influence in shaping our personality. At this level, it is almost indispensable to take recourse in the analysis of Michel Foucault. In his work he dealt with the particular techniques of discipline in modern societies and institutions. He analysed the rise of modern hospitals (Foucault, 1963), psychopathology (Foucault, 1972), prisons (Foucault, 1975) or the history of sexuality (Foucault, 1976). Throughout his entire oeuvre Foucault warns against the reification or objectification of power as such. It cannot be simply seen as mere repression or a particular institution. Power is not only an invasion into the freedom of individuals. It is interplay of forces that have already shaped our concept of freedom. They are ubiquitous and inescapable. Not because they always surround us, but because power itself helps to shape our individuality, which seeks to resist the power (Foucault, 1976).

Foucault’s analysis is even more appropriate in the perspective of Internet environment and the issue of privacy. He invites us not to define abuse on one side and, on the other, the protection of privacy on the Internet as two opposites. Undoubtedly, we enter a play of intersecting forces, which themselves constitute the entire sphere of privacy in the Internet environment. There is not only a counterweight or the result of our actions in the Internet environment, but rather its condition and constantly changing basis.

Summary of the Section

To conclude our philosophical exposition of the concept of privacy, we can note that (1) it naturally springs from our consumerist culture which defies any unproblematic notion of privacy (‘to feel at home’), driving us constantly forward to look for means of identification with others or, more precisely, with their commoditized representations. (2) Nonetheless, this does not prevent us from developing our identity and Internet privacy. We just need to be self-aware and instead of relying on these commoditized forms we should critically appropriate them (therefore the concept of poaching). (3) Our privacy, just as our very subjectivity online (the condition of being an Internet user), is subjected to power and disciplina­tion (of the medium). Therefore, we cannot disengage the protection and violation of one’s privacy. We cannot divide our freedom and determination in the Internet environment; and last but not least, we do not have a shared preconception of privacy as it is constantly reshaped by our actual activities online. Like being on our balcony in slippers and housecoat – while being (potentially) visible to anybody.

Just as a person’s cognitive abilities influence how he or she perceives and approaches the world, so the possibilities of processing personal data of (potential) customers create a broader view of firms on the environment in which they conduct their business and in which their activities take place. It is only at this basis that organizations can make decisions about their future activities, as is discussed in the following part.

THE POSSIBILITIES OF PROCESSING AND USING PERSONAL DATA ACCESSIBLE ON THE INTERNET

Personal data that can be accessed through various Internet-based services (blogs, forums, Facebook, Twitter) can be further processed and evaluated according to the objectives of a company. Personal data in particular are of a great help when analysing a large dataset and segmenting it. For example, the mes-
sages posted in discussion on forum are automatically processed and can be categorized by the sex or the hobbies of the users on the basis of acquired personal data. This way we can see the difference between opinions of women and men or categorize the posts by topic. In relation to the privacy of a subject on the Internet, it is appropriate to mention the basics of the acquisition, processing and evaluation of freely accessible personal data on the Internet, and the fundamental analytic approaches used in company and marketing management. Data can be acquired:

- **Manually.**
- **Automatically:** Data can be put in a database directly or by an artificial actor (softbot) programmed to acquire data on selected web pages or via selected Application Programming Interfaces (API).

In the case of manual data acquisition, an employee goes through each Internet-based service and creates his or her own database (e.g. in a spreadsheet application), which will be later interpreted and used for decision-making. For example, a marketing specialist can register data about the progression of marketing activities (e.g. the numbers of positive and negative feedbacks) which they will use later for the evaluation of marketing activities arranged through various tools (e.g. social media, forums, specialized web portals).

In the case of automatic data acquisition, it is necessary to select data sources and the way of acquiring data. With external data sources, it could be structured data acquired via API interface of a particular service, data acquired by front-end systems (e-shops), or non-structured data from web pages or documents – see the paper (Pavlicek & Novak, 2015) focused on external data sources. The application of a particular method of data acquisition relies on (besides the financial and technological state of a company) a specialist’s conclusion – the resources and time needed to create a program for data acquisition vs. data volume, data processing, the extent of a campaign, future utilization of the data acquired, etc.

Data acquisition is followed by data processing – e.g. data conversion that enables their evaluation by methods used in knowledge discovery in databases (Witten, Frank & Hall, 2011; Rauch, 2013). Pre-processed data are further evaluated – e.g. by a reporting or analytic application (Kliegr et al., 2011), in most of cases with an objective to detect hidden correlations between variables (Pour, Maryska & Novotny, 2012). The results acquired this way must be put into context with other results and further interpreted. It should be considered that even in the case of automatically processed and evaluated data, the results are assessed by a specialist. When non-structured data (e.g. text on a web page without semantics for machine analysis) are processed, the pre-processing of these data is necessary to ensure a fundamental level of understanding of the content by a machine. Recently, the development of Web 3.0 technologies has started. These technologies are designated not only for human, but also for artificial actors, to whom they provide semantical information about the content of web pages. Possibilities of data processing and evaluation:

- **Manual:** An employee may use the tools of a selected office suite and put the acquired data into a table
- **Automatic:** Processing using selected technologies and approaches
  - **Structured Data:** Data available in the databases of particular systems, e.g. Customer Relationship Management (CRM) systems, e-shops or Enterprise Resource Planning (ERP) systems
  - **Non-Structured Data:** Data available mostly on the web or in documents, which need to be pre-processed by Natural Language Processing (NLP) approaches to ensure a fundamental level of understanding of the content by a machine
Among the necessary and the applied techniques for data acquisition and processing for companies are ‘intelligence’ approaches (particularly reporting and analytical applications). In the lead is business intelligence which is ‘a set of processes, know-how, applications and technologies, which are targeted to support effectively and functionally the management activities in a company’ (Pour, Maryska & Novotny, 2012, p. 16). These intelligence approaches amplify the ability of a company to use knowledge assets in action. Similar approaches were developed in other specific areas which affect management on a strategic and tactical level and related activities (e.g. competitive intelligence, marketing intelligence, customer intelligence, media intelligence). The term business intelligence has been used since the 1980s (Bartes, 2010), but similar intelligence systems used by big companies have been in use since the 1970s. As ICT was being developed, including the Internet, an emphasis was put on the acquisition and evaluation of internal and external data related not only to a company, but also to competitive subjects. Thus, Pranjic (2011) considers the two dimensions needed to make the right business decisions: business intelligence (to know yourself) and competitive intelligence (to know your environment, competitive subjects). It is competitive intelligence that allows companies and their brands to be integrated in a specific market environment and a socio-cultural context of particular phases of a company’s or a product’s life cycle. For example, it is very difficult to enter a new foreign market without a deeper understanding of the social, cultural and political environment. Thus, it is necessary to conduct a market survey on the level of competitive intelligence to understand its specifics and to use these pieces of knowledge for the strategic management of marketing activities (Tej Adidam, Gajre & Kejriwal, 2009).

Recent approaches have focused on the analysis of structured and non-structured data; non-structured data are pre-processed and converged to structured data using NPL dictionaries and are further analyzed (Baars & Kemper, 2008). Since we were evaluating non-structured data, we were not able to converge them to structured data absolutely correctly. Nevertheless, the available options are in most cases sufficient for the subsequent data processing. For example, in sentiment analysis (Liu, 2012) we are able to focus on the categories of sentiment, i.e. positive or negative feedback (Sperkova & Skola, 2015).

Some approaches and techniques used in business intelligence and other segments related to knowledge discovery in databases belong to the field of Data science, which is based on data-analytic thinking and data-managed decision-making across the organization (Provost & Fawcett, 2013). The roots of this scientific discipline go back to the 1960s. It is not a system or set of practices as in the case of business intelligence, but there are particular and generally applicable ways of knowledge discovery from acquired data which must be further integrated into specific models. One such example is data processing for predictive analysis. Data science also involves approaches dealing with datasets which are too large to be processed by common methods or systems – so-called big data (Provost & Fawcett, 2013). The processing and evaluation of big data is a current trend in many interdisciplinary informatics fields (e.g. community, humanistic, social or historical informatics) and also in the fields of the medial-communication cycle of science or marketing in relation to the evaluation of online communication or marketing activities.

Processing data available on the Internet is no longer just a challenge, but a reality. Both personal (consumer intelligence, marketing intelligence) and company (competitive intelligence) data is processed for commercial purposes. Apart from that, these data can be used in e-research and other activities which are in the public interest (e.g. security intelligence). We are witnessing a new dynamics and continuous changes in individuals’ views on their privacy, which are influenced by the possibilities brought by ICT. Similarly, this dynamics affects the organizational context of firms (mainly security and communication) and their ability to process enormous sets of data, which has an impact mainly on their marketing and management.
**The Limitations of Handling Private Data in Internet-Based Services**

Information technology and the possibilities of Internet-based services constantly evolve. Almost every online service requires users’ personal data for the possibility of its use. The safety and the handling of these data is a very important issue these days, both for the users and providers of online services – see also *Guide to data protection for public and organization* available at (ICO, 2015). Within the European Union – see (DLA Piper, 2014) – the default privacy principles are primarily governed by the European Directive 95/46/EC from 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The year of its inception suggests that this directive is already quite old and therefore does not reflect the current situation. This directive needs to refine and thereby at least partially reflect current development.

Currently we can mention for example the act from 15 June 2015 when the EU Council approved a general approach to the general data protection regulation. It establishes rules adapted to the digital era and according to that cookies should be included in personal data. The current EU Directive 2002/58/EC on Privacy and Electronic Communications (known as the E-Privacy Directive) obliges member states to adopt legislation requiring a prior approval of the use of cookies. In practice, this means that when you use cookies, which are designed to collect users’ personal data, you need to obtain the users’ consent with the use of cookies on your website.

Besides the refinement and fragmentation of laws within the EU, there is a number of clarifications on the level of national laws – see (European Commission, 2015). This leads to each state having slightly different laws. When doing business in a foreign country, it is necessary to become familiar with the specific legislation of a particular state. The fragmentation of legislation worldwide is even greater. For example, the US laws vary across the individual states, but also with regard to the type of sector and media. In addition, there are often various exceptions.

If we are to summarize the basic principles, the following recommendations for practice can be drawn. User’s consent must be obtained when collecting personal data (i.e. the opt-in principle) for a specific purpose. This purpose should be stated, for example in business conditions. Using personal data for subsequent marketing purposes makes it obligatory to give users the option of cancelling their agreement with the use of their personal data, and thus to ‘unsubscribe’ from a database of respondents. The user has the right to request a statement of his personal data stored by the data manager. He or she can also ask for their personal data to be deleted. The data manager must comply with the user’s request.

**THE NEGATIVE CONSEQUENCES RELATED TO THE ACCESSIBILITY OF PERSONAL DATA ON THE INTERNET**

An important issue is the use and the possible misuse of the freely available personal data that can be manually or automatically harvested by bots (data-harvesting softbot) and further processed by third parties. As an example, It is presented information that can be obtained from the Facebook service, which can be used for human resource management (Bohmova & Malinova, 2013; Benson, Morgan & Filippaios, 2014), marketing (Jasek, 2015), or abused for various forms of (cyber)bullying in a workplace or used by malicious data miners to threaten the privacy of users (Al-Saggaf & Islam, 2015):
Generation Y and Internet Privacy

- **Personal Information**: Belief, orientation, references to family, political opinions, contact information, what the user likes, employment/school, partially also pictures and multimedia content.
- **Information on Location**: Address, current position.
- **Data on Interaction**: A post on the wall, partially pictures and multimedia content, comments.

These data can be (mis)used mainly for unfair marketing practices. On the one hand, these data are used by Facebook itself for targeted advertising. On the other hand, the publicly available data are misused by harvesting and subsequently selling them to third parties. These include e-mail, phone and instant messaging, which can be supplemented with additional information (e.g. physical location) of the subject that owns it and used for targeting in an unfair commercial communications campaign.

Equally important are the social consequences when these data are used by any person for the purpose of discrediting or damaging the reputation of a particular individual. It could be personal data, available posts, comments and pictures, which are a gate into his or her private activities. In the work environment the information can be used for cyberbulling a worker in a particular group. An example: an innocent photo from Facebook can be simply modified and send anonymously to group members. This conduct can have serious implications for team communication and working environment, which is negatively projected into the business activities of the organization. The following types of bullying are specific for a working team:

- **Mobbing**: Bullying by colleagues in a team.
- **Bossing**: Bullying by superiors.
- **Staffing**: Bullying by the subordinates of a superior, with the aim of unseating him or her.

The misuse of selected data (beliefs, political opinions, etc.) along with other forms of pressure – underestimation of work performance, constant criticism, assigning meaningless actions that have nothing to do with the working position or a person’s real character – may amplify the negative effects. These are only some of the problems arising from the use of private information available about a person in the context of an organization and it is only one side of the coin. Concerning our topic, it is appropriate to refer to other resources where authors deal with the consequences associated with data available via social media – (Lashkari et al., 2010; Young & Quan-Haase, 2013; Ibrahim, Blandford & Bianchi-Berthouze, 2012).

Despite these potential dangers and possible negative consequences, today’s young people leave in the Internet environment reflections of their daily activities, which together with other personal data present new possibilities for individual or personal online address. It is not only companies offering services to their customers, which can carry out a better segmentation of their customers and individually address them thanks to this information (Sperkova & Skola, 2015; Jasek, 2015). It is also for those who want to exploit a person – gaining control over their e-mails or identities and their potential future misuse, for example for botnet attacks (Boshmaf et al., 2013), gaining the trust and then manipulating a person in order to carry out certain actions, obtain certain information (e.g. credit card numbers) and disclose their secrets (Hadnagy, 2010). On the one hand, this provides greater comfort and thus better meets people’s needs (connected with a better segmentation of customers), and on the other hand, there are risks that cannot be underestimated on the personal (gaining control over online identities, manipulation, etc.), organizational (disclosure of company secrets, cyberbulling in workplace) or societal level (ethics, different approach to privacy).
GENERATION Y’S PRIVACY SETTINGS IN SOCIAL NETWORKING SERVICES

After an overview of topics related to Internet privacy and the possibilities of the acquisition and processing of the data of the users of Internet-based services, we focus on the results of relevant research studies. We start with own research (Cermak, Smutny & Janoscik, 2014), in which we compare the approaches of young people (age 15-30) from France and the Czech Republic. In this survey, such differences in behaviour are accentuated that originate in the cultural specifics of each country. This section also includes other interesting results from relevant surveys focused on Internet privacy. The conclusions following from these studies will enable companies to create their own strategy for obtaining information about customers and their interactions – e.g. for the purposes of marketing and management. This concerns mainly the different tendencies of young people in different countries to publish certain types of personal data, which can then be automatically processed; and the elements that motivate a person to give away personal data of their own free will.

The survey (Cermak, Smutny & Janoscik, 2014) presents two perspectives on privacy in the social networking services, both from a theoretical and a philosophical point of view, as well as from the perspective of practical research on the social network Facebook. The aim is to synthesize those views and discuss the positives and negatives of the actual phenomena occurring in this environment during social interaction.

In total, we analysed 531 Facebook profiles of people aged 15-30 years. For each profile was gathered visible data in two cases. The first was the visibility of data from the perspective of a friend (i.e. we explored the account from a profile which was in the friends list). The second was the visibility from the perspective of a random user of Facebook, i.e. the user who was not included in the circle of friends in the monitored Facebook account. At first, we introduce the answers to the three main research questions of this study, which will be followed by a discussion:

- **What kind of information is most frequently freely available?** The most freely published data are name, gender, friends, liked pages, current location, school/university and posts on the wall related to personal experiences, posts containing entertaining content and comments on current events – i.e. the data of general character. In contrast, data containing contact information, such as address, phone number or e-mail and data relating to personal beliefs (religion, political beliefs) are published with the least frequency.

  Interestingly, users from France do not publish their true name in more than a quarter of cases. They use a profile under a different name or nickname. But (unlike Czechs) the French frequently publish their e-mail address, date of birth and information about their current location and hometown. Czech users disclose more information about their current school/university, as well as about their friends and the pages they like.

- **What information is most often available to friends but hidden to other users?** When comparing the differences among public and private data available in each country, the most significant differences were found out in posts on the wall, date of birth and photos presented on Facebook. In the Czech Republic, there is a difference of about 70% (for example 96% of users from the Czech Republic make posts from personal life available to their friends, but only 23% to general public), in France it is about 50%. Approximately a 40% difference was found in data relating to family,
employment position, e-mail, school and the pages that the user likes. For these data the differences are more or less the same for users from the Czech Republic and France. The most significant differences in data availability between France and the Czech Republic relate to the current employment position (33%), funny posts on the wall (28%), information about the user (25%) and published pictures (25%).

- What is the most frequently shared information on the wall of Facebook in each country and is the information only visible to friends or to other users as well? In the case of public posts, the French frequently publish posts about their personal life, work and past events. Czech people make more often available to public only the posts with funny character, compared to the French. In the case of posts published for a circle of friends, majority of Czechs and the French write on the wall posts from their personal life. The differences can be found in other types of posts. Czech people more often than the French publish on their wall posts commenting current events (news) and posts that are funny. On contrary, the French publish more posts associated with their employment. Overall, Czechs publish their posts frequently only in their circle of friends, while the French often leave their posts freely available.

Results from the evaluation of publishing pictures and information about friends and favourite websites show that in the case of friends, the information is more often published by Czech users in all cases. It is the same when publishing for the general public, except for pictures, which are more frequently published by the French.

With regard to the philosophical basis outlined in the background section, we can continue with a particular archaeology of subjectivity in the environment of social networks on the Internet. Based on our data collection, there is an obvious difference not only in the actual administration of users’ personal data, but also in their relationship to the network as a whole. While French Facebook users show more effort to protect their information in general, in the case of the key items in relation to the profile on the network and their real lives, the opposite is true. Despite a greater tendency to publish a large number of surveyed items, Czech users very strictly protect information that makes them identifiable at other levels (phone number, email, location). For most of these items, the publishing rate by Czech users is around 1%, some items such as telephone number or zip code are not published at all. As opposed to a premature conclusion that could only quantitatively evaluate French privacy, we provide a more accurate insight. Differences in the data indicate rather a different role that the social networking services plays. In France, the network is more tightly linked to other layers of identity of the users. This naturally puts pressure on a better control of the published data. In the Czech Republic, social networks follow first the logic of remediation – rather than create a supplement to real identities, so they act as an alternative to real identities: social networking services is a space in which the users do not follow their identification data but rather generate new relationships on media basis. This can explain the lower pressure on protecting the remaining items of personal data that are involved in the creation of an alternate reality (e.g. status, friends, favourite pages).

The survey results are therefore consistent with the philosophical basis. (1) At the level of criticism of consumer culture, we can use Adorno’s conceptualization of the attack on privacy in data analysis. This happens not only through the threat of misuse, but from the opposite side by putting pressure on the publishing of personal information by a user. (2) At the level of media reflection along with De Certeau, we see that the media (in our case the social networks) extend the possibilities of user behaviour in relation to their data, but do not add autonomy of their users. Media logic penetrates the user’s
Generation Y and Internet Privacy

imagination, forms ‘his fears, his dreams, his fantasized and lacking authorities’ (De Certeau, 1984, p. 176) and thus also his or her idea of privacy. (3) We can expand together with Foucault these media penetration mechanisms into individual ideas. He tries to conceptualize the phenomenon of power not as a substance or a centre, which attacks our individuality, but as the fabric of the network which helps to create it, including our ideas about privacy and its protection. In the study of outlined power we cannot only monitor cases of penetration of privacy. It is necessary to describe and assess the acts of users themselves, who are always already shaped by that power relation.

In general, we can summarize that the social networks on the Internet are at a very specific level at which the individuality of the user interferes with the invasion of transpersonal structures, which are characterized here:

1. Their mass,
2. Media logic, and
3. Nature of power.

Naturally, this issue calls for a specialized interdisciplinary elaboration. It can not only provide the analysis, description and evaluation of the dangers that are hidden in the accessibility of personal data published by users, but it also develops some considerations (based on Adorno and Foucault) about the development of the human personality in today’s dynamic environment. Although the survey is relatively limited and the comparison is only bilateral, the authors consolidated the general perspective on how to approach the issue of privacy on social networking services.

The afore-mentioned research will now be supplemented with the results of other relevant inquiries. Let us begin with (Syn & Oh, 2015), who confirm the diverse motivations for sharing private information within social networking services. These depend on demographic characteristics, experience with these services and Internet usage, as well as the characteristics and features of the services themselves. Users could be highly motivated by the learning and social engagement aspects of social networks.

Different attitudes can be found even among men and women. The latter are prone to a proactive privacy protection behaviour on social networking services and generally in a Web 2.0 environment than it was reported around the year 2000. Almost a half of both genders are not aware of how personal information is being used (Hoy & Milne, 2010). However, results from the research study (Benson, Sari-dakis & Tennakoon, 2015) show that control over personal information published in social networking services is negatively and statistically associated with information disclosure. Both user awareness and security notices have a positive statistical effect on information disclosure.

Another research (Cecere, Le Guel & Soulie, 2015) conducted in 26 European countries verifies that the conception and awareness of privacy is positively affected by national policies concerning personal data protection, which differs in individual countries. Similarly, it asserts that cultural and socio-demographical variables affect the level of concerns one has about his or her privacy online.

Although privacy is valued for many reasons, as was mentioned about Generation Y, who take the Internet as an integral part of their lives, this issue is still not taken seriously (Al-Saggaf & Islam, 2012). The educational programs currently implemented point towards information and security risks (Kolin, 2011), but this process started relatively late and it affects rather the Generations Z and Alpha, not the Generation Y, which currently becomes economically active. Another problem presents the relatively weak and fragmented support in the legislation of particular countries concerning possible misuse of personal data (Al-Saggaf & Islam, 2015). Nonetheless, we can consider the efforts taken by the social
network providers themselves, in order to maintain the anonymity of their users using their particular services, as positive initiative (Wang et al., 2015; Rajaei, Haghjoo & Miyaneh, 2015). Despite that, the technological possibilities of misuse of available data has technologically advanced further than the options of both direct (technological) and indirect (awareness, proactive attitude of individuals) protection of user privacy.

On the other hand, social networking services make possible a leak of private information as observed by another study (Li et al., 2015) focused on Facebook, Google+ and Twitter services. This stems from the conflicts between privacy control and social networking services functionalities. Besides online social networking services themselves, we can observe the games played via social networking services. According to existing research (Chae & Lee, 2015), the attitude of users towards privacy in specific social networking service does affect their perception of advertisements within the games. Primarily, these games use the identity of a user to address his or her friends. Despite the fact that social networking services have been successful in limiting the risks of direct access to personal data, the danger resides in communication through the profile of a player, which can be seen as unfair marketing communication. These findings confirm our philosophical exposition of the problem of privacy in which we have argued against the extrapolated scheme (privacy versus intrusion) in favour of a more holistic view in which the privacy is not intruded but rather formed by the online social networks.

There is significant group of users who are aware of the potential dangers of personal data being accessible through various social media. Nonetheless, these negative aspects are in many cases outweighed by certain benefits. Existing research (Min & Kim, 2015) introduces three enticements: the motivation of relationship management through social networking services, the perceived usefulness of social networking services for self-presentation, and the subjective social norms of using social networking services. ‘The results regarding the positive and negative effects of suggested benefit and cost factors on information disclosure show that only the combined positive effects of all three behaviour enticements exceed the negative effect of privacy concerns, suggesting that privacy concerns can be offset only by multiple benefit factors.’ (Min & Kim, 2015) Possible threats connected to social networking services affecting users, including the means of their prevention, are listed here, for instance (Fogues et al., 2015).

SELECTED FUTURE RESEARCH DIRECTIONS AND ISSUES

Within the reflection on future paths of research and development approaches to Internet privacy it is necessary to offer once again the perspective of two levels – personal and organizational. If we begin with the personal level, we have to highlight the increasing global information and security literacy even among the representatives of Generation X and Y. On the other hand, new technologies still emerge. Consequently, these technologies bring new perspectives on privacy and also remake old approaches. We should mention mainly the services based on Web 3.0 and ubiquitous technologies.

In the case of Internet-based services built on the Web 3.0 technology, which focus mainly on the semantization of content on the Internet for artificial actors, there are new ways of influencing the subjectivity of the human user by the behaviour of artificial actors. Because of the fact that Internet-based services are not user-tailored only to people, but will also be readable for softbots, it can be expected that even the artificial actors will enter into relationships with human actors and will influence their subjectivity. Artificial actors and their actions will thus affect human subjectivity more than now – see also the marketing concept of the management of subjectivity (Firat, 2014; Tadajewski & Jones, 2014).
For example, an artificial actor can seek and reach a human (at a similar level of communication as another human) who has a specific mix of interests, establish a relationship with him or her and influence them by its contributions. In the context of Internet privacy, this is an issue of the selective approach of artificial actors to personal information, primarily within a field of social networking services. In other words, we can distinguish between good softbots (e.g. indexing Googlebot) which increase attendance and bad softbots which abuse the personal data for the needs of their maker.

Ubiquitous technologies develop at the level of both physical and virtual environments (e.g. the terms as the Internet of Things, Internet of Services) as well as on the level of mixed reality. In the area of social networking, future development is associated with the development of ubiquitous social networking that will support the social wellbeing of people in their everyday lives. This means a diversion from the centralized web-based social networks and the transition to ad hoc social networks that are limited by certain physical areas, where they promote social interaction. Although there are not many real applications, an important aspect of these technologies is privacy – controlling the access to personal data (Sapuppo & Seet, 2015). A current trend is the development of general models that deal with specific problems associated with ubiquitous technologies – e.g. (Chikhaouia et al., 2014; Lopes et al., 2014; Pesout & Matustik, 2012).

From the perspective of organizations and the usefulness of freely available data on the Internet, mainly for marketing activities, current development focuses on the identification of customers through various Internet-based services. The aim is to identify the different identities (e.g. profiles on Facebook or Twitter) as one customer, which will contribute to a better monitoring of customer behavior (their web traffic), the individualization of services and enhancing marketing models working with customer data such as customer lifetime value or electronic word-of-mouth analytical models (Jasek, 2015; Sperkova & Skola, 2015; Cheunga & Thadani, 2012). First studies concerning this identification are currently available – see (Long & Jung, 2015) – which for this purpose process available (personal) data. Let us add that this task may become easier in the future if Web 3.0 technologies are fully enforced.

Although companies focus their attention mainly on the processing of internal and external data (of their customers), they are at the same time caught in a trap created by their problems (inability) with processing large amounts of data from a wide variety of structured and unstructured sources. For instance, according to a survey among Czech small and medium-sized companies (Smutny, 2015) the results show that the fundamental problems perceived in connection with the processing of data from the Internet for marketing purposes are in particular:

1. Increasing time demands associated with the use of a large number of tools and services (e.g. social media, advertising systems).
2. The inability to create a holistic view of the success of their marketing activities. Currently, they rely only on partial instruments providing individual statistics.

On the other hand, it should be noted that only a small proportion of companies from Central and Eastern Europe (contrary to Western Europe and the USA) is pressed by competition to increase their use of potential data sources, or rather to a synergistic use of online marketing tools (Janoscik, Smutny & Cermak, 2015; Smutny, 2015).

The issue of Internet privacy is closely associated with technological development as well as with information literacy of the users of Internet-based services – i.e. the awareness of the risks associated with the availability of personal data, especially within the group of users of social networking services.
Generation Y and Internet Privacy

As stated above, there is a large number of empirical studies dealing with the approach of Generation Y to self-disclosure, including the phenomena supporting this sometimes risky behaviour. From the perspective of firms, there is a trend to increase economic efficiency by supplying current marketing, data-driven and others models with qualitatively new data (Pavlou, 2011). However, this trend, in our opinion, is slowed down by a related problem, which is the lack of technological and expert resources within companies (Maryska & Doucek, 2012) that would enable carrying out the gathering and processing of available data at the required level.

CONCLUSION

This chapter brought up an array of topics directly attached to Internet privacy both from the perspective of a regular user and from that of commercial organizations. This view from both sides can provide companies with better understanding of various aspects of Internet privacy. Our main concerns with generational and cultural differentiations, philosophical scrutiny, possibilities of data acquisition and analysis, legal framework, and negative consequences of personal data availability, all these aspects do intersect and form a basis, on which we can articulate other ideas focused for instance on prospective usage of personal data available on the Internet with the emphasis on the needs of firms. On the other hand, it was addressed even the issues of their misuse in personal and organizational context (manipulation of users, security risks etc.).

In order to understand the contemporary behaviour of Generation Y and their attitudes towards self-disclosure through social networking services we have discussed our preceding comparative research in its wider system-oriented framework and based on selected set of other studies. In concluding parts we have provided not only important findings of recent research concerned with young users of social networking services and their treatment of their personal data.

We discuss even some prospective technological trends, but also some problems involved in economic interests of companies. In this respect the chapter outlines basic directions for companies to set and realize their activities connected with usage of freely available (personal) data. These might be outlined as consolidating available means of data sources, using analytical approaches (e.g. business intelligence) and models (e.g. customer lifetime value, electronic word-of-mouth) and secondly clear set of ethical principles of work with personal data including legal integrity. These courses of action are essentially dependent on technically educated employees and technical possibilities of particular company.

The most important implication for company practice can be summarized in the following points:

1. In companies’ effort to acquire data for their marketing and management activities through Internet-based services, it is necessary to motivate people to provide personal data of their own free will (e.g. special commercial offers, discounts, presents, promo actions, individual approach). Different generations (and target groups) have a different understanding of privacy and tendencies to self-disclosure. Privacy is not intruded but rather formed by social networking services. This way of acquiring personal data seems to be more fair, as opposed to e.g. harvesting personal data from selected websites without involving their owners.

2. Cultural and generational differences are reflected in social interactions via social networking services, but also in a preference for certain products or services and thus a demand for them. Every culture or country has a different set of values, which are reflected in the feedback or reactions
of people on media and marketing communication activities. Connected with that is the Agenda-
Setting Theory, i.e. the ability of mass media to influence the audience and suggest topics which
are then further dealt with via social networking services.

3. The Glocalization principle needs to be applied in the current Internet-mediated environment mainly
for cultural and geographical reasons. This means adapting globally offered services and products
on a defined local level (e.g. continent, country, language group), and their specific conditions (see
Hofstede’s cultural dimensions theory).

4. In the same spirit it is necessary to consider different aspects when targeting marketing activities
(market segmentation). Those include generational (every generation has different needs, priorities,
the ability to use modern technologies) and the above-mentioned cultural (the tradition of an
established brand, established schemes and product types) specification of a particular group.

5. A problem connected with privacy is that of security and decreasing the danger of a leak of sensitive
company data, which happens mainly via company employees. The basic solution is to limit access
to individual data sources of potential information according to objective information requirements
of a certain position.

6. When using social networking services on individual or company level, it is necessary to con-
sider possible (mis)use of the published information, for example by business rivals (e.g. as part
of competitive intelligence, targeted damage by unfair communication campaigns). Data can be
automatically processed by softbots, which will increase further with the gradual supplication of
Web 3.0 technologies.

Let us also mention two current technological trends with a great social impact that are connected
with the continuous development of ICT and mainly social networking services, which will in the near
future affect the majority of companies doing business over the Internet:

1. The development of Web 3.0 technologies and mainly the semantization of webs will lead to more
effective use of artificial actors (softbots), which will no longer process only unstructured data, but
more often rather structured data freely available on the Internet. Other artificial actors with their
profiles on social networking services will then be able to affect human subjectivity – even now it
is very difficult e.g. on Twitter to determine whether a profile belongs to a human, a softbot, or a
human acting like a softbot. It can therefore be expected that there will be a massive use of various
forms of artificial actors, for instance for marketing, communication or competitive activities of
firms. This issue concerns not only collecting and processing available personal data, but mainly
the direct effect on a person’s subjectivity and thus also on their perception and understanding of
certain topics (including their attitude to privacy).

2. The expected development of ubiquitous technologies brings also the so-called ubiquitous social
networks. Ad hoc social connections will be established within a certain area, which again con-
cerns the issue of privacy. This technology will affect mainly retailers in stores, who will have new
possibilities for propagation thanks to localized social interaction. For a better idea, let us give an
example: A person walking in a street will be notified via his or her mobile device (on the basis of
their interests, age, recent social activity) about a relevant shop located nearby. If interested, this
person will be able to see their current offer (e.g. he or she is motivated by some discount if he or
she makes a purchase there during the following hour).
Nonetheless our excursus into the problem of Internet privacy has not been limited to exposing and discussing basic issues, risks and prospectives. Mainly due to our philosophical grounding we have critically reassessed the very notion of privacy after our massive experience with social networking services. We need to think about their impact on our private sphere neither in terms of intrusion nor with some preconceived understanding of what privacy actually is. By no doubts it is being rearticulated and not only distorted by new technological means. Moreover there is no unequivocal private sphere since the publicity on social networking services capitalizes precisely on exposing our personal data. Like being on our balcony; on one hand confined to our private household, and on the other hand being completely exposed (Arendt). Nonetheless even this irritating situation has its prospective courses of action. Firstly we need to be aware of this exposure (Adorno). But this does not prevent of from reaching into this metaphorical space of social networks. We just need to appropriate its consumerist background and turn it into more critical “alterconsumerist” approach (De Certeau) admitting our very privacy to be informed by the networking (Foucault).

REFERENCES


Generation Y and Internet Privacy


Generation Y and Internet Privacy


**ADDITIONAL READING**


Generation Y and Internet Privacy


ENDNOTES

1 Subjectivity can be understood as the condition of being an Internet user. Human subjectivity is individual experience, which is always unique and influenced by the environment and the actors in the environment (in the Internet environment, these could be human but also artificial actors) in which the subject resides.

2 This chapter was prepared thanks to the same research project VSE IGS F4/18/2014 at the University of Economics, Prague.