UDC 004.735.5:004.056
Original Scientific Paper

Online privacy: overview and preliminary research

Renata Mekovec *renata.hudek@foi.hr*
University of Zagreb
Faculty of Organization and Informatics Varaždin

Abstract

Over the last decade using the Internet for online shopping, information browsing and searching as well as for online communication has become part of everyday life. Although the Internet technology has a lot of benefits for users, one of the most important disadvantages is related to the increasing capacity for users' online activity surveillance. However, the users are increasingly becoming aware of online surveillance methods, which results in their increased concern for privacy protection. Numerous factors influence the way in which individuals perceive the level of privacy protection when they are online. This article provides a review of factors that influence the privacy perception of Internet users. Previous online privacy research related to e-business was predominantly focused on the dimension of *information privacy* and concerned with the way users' personal information is collected, saved and used by an online company. This article's main aim is to provide an overview of numerous Internet users' privacy perception elements across various privacy dimensions as well as their potential categorization. In addition, considering that e-banking and online shopping are one of the most widely used e-services, an examination of online privacy perception of e-banking/online shopping users was performed.

Keywords: online privacy, privacy perception, e-banking, online shopping

1. Introduction

In the online environment, a major problem for users who have become an object of surveillance is the possibility of their identification. Furthermore, for ordinary Internet users it is difficult to identify the companies which are monitoring their online activity and to determine the way in which user surveillance is carried out. While they visit a web site in order to browse for information, make a purchase, or communicate with others, it is difficult for users not to leave trace of their online activities.

In many cases the web sites request the users to disclose their personal information. After collecting this information, web sites may offer their users benefits or personalized environments, ranging from discounts and data access for registered users to a welcome message with the user's name that pops up when the user visits the web site. Internet users are therefore often faced with the cost-benefit dilemma of choosing between the commodities granted for disclosing the requested personal information and possible negative consequences of personal information disclosure. Among the issues related to negative consequences of personal information disclosure in the online environment, the online privacy issue is by all means one of primary importance.

New Internet-based technologies are not only increasing the capacity for collection, processing and usage of users' personal information but are also changing the dynamics surrounding the collected information and privacy protection. Easier identification of individuals is another relevant issue that has arisen [42]. Users' Internet actions like visiting web sites, purchase and disclosure of personal information can all be categorised as privacy-related customer behaviour [20]. In addition, a lot of Internet users are confused and do not

know what their online privacy protection rights are. Moreover, they are not acquainted with possible ways of online privacy protection [39].

Privacy has long been seen as a multidimensional concept where some of the most referred privacy dimensions were [4]: (1) information privacy; (2) physical privacy; (3) social privacy; and (4) psychological privacy. In the Internet environment the problem of information privacy is perhaps the one to have been highlighted most. Users' concern for their online privacy is based on the fact that they want to be able to control the collection, storage and usage of information about their online activity. Major attention is given both by the users and by the media to various types of personal information misuse, ranging from spam and online marketing activities to more dangerous ones, like identity or credit card theft.

Privacy appears to be one of the main factors that influence users' behavior on the electronic market [6]. The concern for appropriate collection and usage of users' personal information has been increased due to the development of e-commerce [32]. In order to fully use the potential of e-commerce it is important to accurately understand Internet users' concerns for their information privacy [23].

An overview of recent literature revealed that most of the authors focus on *information privacy issues*, i.e. on personal information that online users consciously or unknowingly disclose to a web company. As this particular area of research is quite specific, other privacy dimensions should not be ignored. Physical privacy refers to individual's right not to be supervised (in his private space). Social privacy applies to individual's right to avoid unwanted communication and to have the right to intimacy and security. Psychological privacy refers to individual's right to be able to express his opinion, feelings and beliefs without any pressure and interference. His overall concept of online privacy can be influenced by his perception of the degree of (1) supervision, (2) intimacy, (3) security and (4) freedom to express his opinion in online environment without negative consequences. In addition, it was noted that only a limited number of researchers investigated various factors of users' *online privacy perception*. This article will therefore be aimed at multiple and diverse aspects of Internet users' privacy perceptions and not only at those related to the information privacy dimension.

There are several important and justifiable reasons to investigate and understand the various aspects of Internet users' privacy perception: (1) number of Internet users is increasing every day and Internet is becoming the most popular communication media, (2) understanding of Internet users' privacy perception will help online organizations to customise their web sites to be more privacy-friendly, (3) based on this understanding the development of new e-services could be improved, and finally (4) it will help to decrease Internet users' resistance to disclosing personal information and consequently will encourage the usage of various e-services.

The article is organized as follows. In section 2 privacy issues regarding privacy in online environment are introduced. In section 3 the categorization of diverse factors that influence users' online privacy perception is proposed. Section 4 presents a research model of users' online privacy perception. According to statistical data e-banking and online shopping are the most widely used e-services. Therefore, online privacy perception of users who shop online or who performed bank transactions is examined. Conclusion is given in section 5.

2. Privacy in Online Environment

Online privacy researches can be divided into two broad domains. The first domain is related to *users* (e.g. the measurement of their online privacy concerns, investigation of situations and factors that influence users' personal information disclosure to the web site, etc.). The second domain encompasses factors that are related to users' environment, including ethical, legal, regulatory, and public policy factors [41]. It must be noted that privacy protection was initially related to one's understanding of privacy as well as to technology improvement and development [34].

In e-commerce customer privacy is viewed as a multidimensional concept encompassing a number of specific issues [10]. Privacy concern of an individual is more an attitudinal than a behavioural factor [5], but the perception of privacy can influence customer online behaviour [7].

When analyzing privacy on the Internet, different types of customers' Internet activities need to be considered. The respective relations between privacy concerns and customers' commercial, informative and communicative online activities can not be treated in the same way [38].

Moreover, when discussing privacy on the Internet in general, it is important to consider whether the increased capacity of customer personal information collection, processing and usage is perceived as a problem by the customer and, if so, to what degree. Chellappa [8] defines perceived privacy as 'the subjective probability with which customers believe that collection and subsequent access, use and disclosure of their private and personal information is consistent with their expectations'. However, this author emphasizes that, when transactions occur in the online environment, it is not only customers' *personal* information that is collected, but also the information about their *preferences regarding information browsing and online shopping.*

The perceived *privacy level* when using the Internet influences the online behavior of individuals. As far as they believe that their privacy is secured during their interaction with a particular web site, users will not hesitate to proceed with the desired transaction or return to this web site in the future. On the other hand, some researchers report that even when Internet users indicate a high level of online privacy awareness, like when they are required to disclose personal information to accomplish a desired transaction, most of them will not hesitate to potentially undermine their own privacy by fulfilling such a request (see: [35], [42]).

Methods for identifying and quantifying personal privacy concerns are important as they enable the online customer behavior to be analyzed [8] and privacy in the online environment to be more precisely defined, so that users' privacy concerns can be studied in more detail [31]. Accordingly, there is a need for a systematization of factors that influence Internet users' privacy perception so that they can be more effectively measured, compared and investigated regarding their interdependence. The results of research based on this kind of systematization of online privacy perception factors can be useful for web companies that offer various services on their web sites. Drawing on these results, web companies could improve, modify or even abandon certain services. On the other hand, policy makers will benefit by acquiring some understanding of the factors that shape and influence consumer online behavior.

3. Online Privacy Constructs

In this chapter the factors that influence customers' online privacy perception will be discussed. Based on former research of privacy in the online and offline environment, privacy measurement and connection between privacy concerns and customer behavior, a number of factors were identified that have influence on customer's privacy concerns. The research described in this article will predominantly focus on e-commerce privacy issues. In order to include factors from all aspects of privacy a factor categorization is proposed. It is based on the following groups which organize the various factors that influence the Internet users' privacy concerns [6]:

1. customer-intrinsic factors;
2. customer perceptions, beliefs and attitudes toward direct marketing and/or in-home shopping, trust, mechanisms for information control, and processes of data collection;
3. web site related factors;
4. situational factors.

According to some authors, besides the four groups of factors proposed above, one or more other groups (of factors) can be conceptualized that are related to *legislation and government protection* (see: [10], [22], [29]).

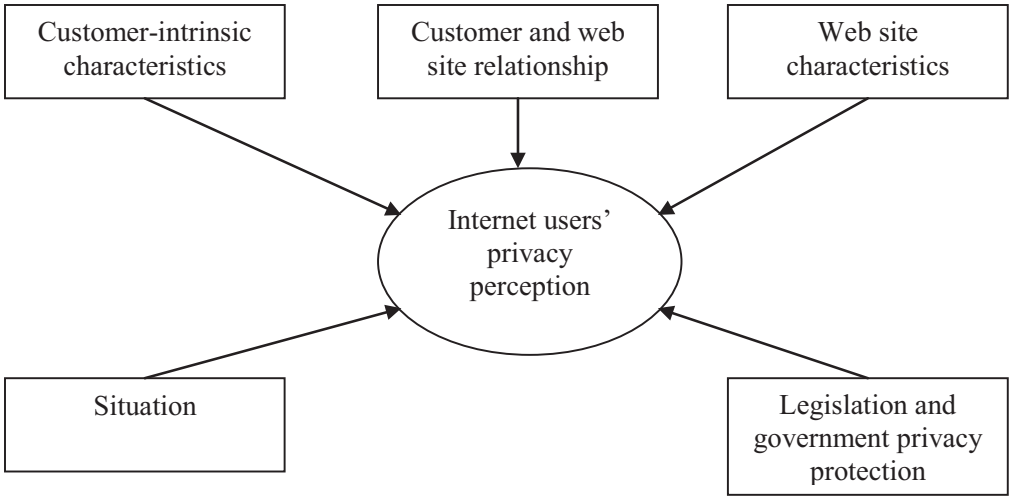

Figure 1. Online privacy factors that influence overall privacy perception of Internet users

In consistence with the former categorizations, for the purpose of this article, the factors that influence the overall perception of Internet users' privacy will be categorized in five groups (presented in Figure 1). The factors that influence the Internet users' privacy concerns will be described in detail in the following sub-chapters.

3.1. Customer-Intrinsic Factors

This group of online privacy factors consists of factors that are specific for individual Internet users. Every Internet user perceives the content and services of a particular web site differently. Therefore, when reviewing factors that influence the Internet users' privacy perception it is important to consider characteristics of users themselves. Besides *demographic characteristics* like gender and age, this group also encompasses the following factors: *education* (see: [10], [23], [33]), *Internet experience* (see: [21], [23], [28]), *privacy segmentation* (see: [10]); *privacy victim* (see: [10], [23]).

Along with the Internet users' demographic characteristics, their Internet experience and education are also important for their privacy perception. There is an assumption that the level of online privacy concerns will be *decreased* if the user has longer Internet experience [28], and also that it may be *increased* if a user has a lower level of education (hypothetical research question, see: [30]).

The factor *privacy victim* refers to Internet users' having been faced with privacy invasion while using the Internet. Privacy invasion implies that the user has been exposed to 'search and seizure, unsolicited e-mail (spam), defamation, creation of databases consisting of personal information and secondary usage of that information' [7] by a third party. It should be emphasized that in this respect privacy invasion refers to situations in which users' personal information is collected and used without their knowledge or approval. Individuals who have been victims of privacy invasion during their usage of the Internet are usually more concerned about their privacy and also will more likely actively protect their personal information [10].

The *privacy segmentation index* is a tool which divides users into three groups depending on privacy sensitivity: (1) privacy fundamentalists, (2) privacy pragmatists and (3) users not concerned about their privacy [10].

3.2. Customer and Web Site Relationship

The relationship between the customer and a commercial web site is predominantly associated with Internet users' *general attitude* toward the processes and ways of collecting personal information by the web site. These factors are related to the customers' perception of information privacy.

The factors observed in this group are labeled differently by various authors:

- access (see: [21], [32]) – refers to customers' right to access to personal information a company collected about them during their interaction via the company's web site;
- improper access (see: [23]) – companies that collect information about their customers have the obligation to protect the information collected from their customers from improper access (both inside and outside the company);
- awareness of privacy practice (see: [23]) – refers to customers' awareness and understanding of the practice that the company they interact with through the web site uses regarding the collection, storage and usage of their personal information;
- choice (see: [11], [21], [32]) – if a company wishes to use the information collected about its customer for other purposes (not approved by the customer) or share this information with a third party, customers' approval should be requested;
- control (see: [6], [23]) – by disclosing their personal information to the company, customers are exposed to the risk of losing control over their personal information;
- collection (see: [23], [33]) – refers to customers' awareness that during their online activity information about them is collected with or without their permission;
- information usage (see: [10], [33]) – during their online activity customers are not only concerned about the collection of their private information, but also about the ways in which that information will be used;
- errors (see: [23]) – refers to customers' concerns about errors in the company's database including the information the company has collected about their customers;
- notice (see: [21], [32]) – companies that collect information about their customers have the obligation to inform customers about the type of information collected, the way in which the collected information will be used and whether the collected information will be shared with a third party;
- privacy attitude (see: [5]) – refers to customers' general attitude regarding privacy when they are interacting online;
- security (see: [21], [32]) – companies that collect information about their customers have the obligation to ensure security during the transmission of customers' information as well as to provide security of the collected information stored in their databases;
- unauthorized secondary usage (see: [23]) – companies that collect information about their customers must protect the collected information from unauthorized usage;
- the *what* dimension (see: [13]) – refers to personal information that companies request from online customers in order to proceed with the transaction;
- the *when* dimension (see: [13]) – refers to a particular moment when the online customer exchanges the requested information with a web site and the period in which the collected information will be used;
- the *where* dimension (see: [13]) – refers to the web site form where online customers disclose their personal information;
- the *who* dimension (see: [13]) – refers to the company that owns a particular web site and collects customers' personal information;
- the *why* dimension (see: [13]) – refers to the purpose of customers' personal information collection;
- the *how* dimension (see: [13]) – refers to ways in which customers' personal information collected by a particular company will be used.

The observed factors will be discussed in more detail in the following paragraphs.

The factor *access* defines that customers have the right to access the information collected about them, as well as the right to change and delete it (see: [32], [21]).

Improper access refers to the protection from unauthorized access to customer information collected by companies during their transactions [23]. Companies should protect customer information from unauthorized access (referring to people both inside and outside a company) within the process of transaction and storage of information [32].

Awareness of privacy practices refers to the level of customers' concern about organizational practice regarding information privacy (information collection, storage and usage). It is related to the users' understanding of organizational conditions of actual practice regarding collected data [23].

The factor *choice* specifies that customers have (1) the right to choose if the information related to them collected for a specific purpose can be used for other purposes and (2) the right to choose whether the collected information related to them will be shared with a third party. According to this factor, companies should ask for customers' approval to use the collected information related to them for other purposes and share the collected information with a third party [32]. To fulfil the conditions stated under the variable *choice*, companies offer *opt-in* and *opt-out* mechanisms [11]. *Opt-in* requires that companies get approval from their customers regarding the usage and dissemination of the information collected about them. *Opt-out* requires that the customers take action to protect their personal information.

Control is a very significant factor in the information privacy context because users are exposed to the risk of losing control over their personal information when submitting personal data. Therefore this factor can be defined as the freedom to express one's own opinion regarding the approval of personal information collecting, namely, to choose whether to approve the collection or to exit [23]. Castañeda and Montoro [6] use two online privacy dimensions: (1) control over the process of collecting and (2) control over using personal information on the Internet. They define the control over information collecting as the Internet users' perception of the control they have over automatic information collection or transmission over the Internet. This factor covers the users' knowledge of the mechanisms for data gathering as well as their right to be informed about different practices and ways of web sites' data collection processes. The control over the use of information refers to 'the level of restrictions imposed by the customer on the use a web site makes of the information collected on him'. According to Milne and Rohm [26], in order to be able to control their personal information, users need to be aware of the information collection processes as well as of the mechanisms that allow information collection restriction (*opt-in* and *opt-out*). Owing to their similarity, the variables *choice* and *control* can be merged into one construct.

Collection represents the degree of customers' concern about the amount of specific individual information on them owned by the other side in relation to the value or benefit obtained in return [23].

If users' personal *information is used* only for transaction purpose, users will not be concerned about their privacy [33]. Individual willingness to disclose private information to a web site depends not only on the type of the information collected but also on the ways information is collected, used and stored [16].

The factor *errors* is related to the errors in the data that companies have collected about their customer, like mistype, inaccurate or outdated personal information [23].

According to the factor *notice,* users have the right (1) to know if a specific web site is collecting information about them and (2) to be informed about the way in which that information will be used. Companies should notify their users about what specific information will be collected, how the site can use them for internal purposes and/or share it with a third party [32]. Owing to their similarity, the variables *notice* and *awareness of privacy practice* can be merged.

Buchanan et al. [6] developed an instrument for measuring the customer *privacy related attitude and behaviors*. The instrument consists of two dimensions: (1) privacy behavior and (2) privacy attitude. The dimension *privacy behavior* describes the customers' ways of privacy protection and the dimension *privacy attitude* reflects the customers' general attitude regarding privacy when they are online.

Security defines that online companies should take some steps to provide security during the transmission process as well as to provide security of the received information stored in their databases [32].

Unauthorized secondary usage refers to the unauthorized usage of personal information that online companies have collected about their customers [23].

Harkiolakis [13] presents a *six-dimensional approach to online privacy*: what, when, where, who, why and how. The '*what'* dimension refers to personal information that is requested in an interaction. The '*when'* dimension covers the time when the information is collected and the period during which the collected information will be used. The '*where'* dimension is related to the web site form. The '*who'* dimension is concerned with the company collecting customers' personal information. The '*why'* dimension refers to the reasons for customer information collection. Finally, the '*how'* dimension corresponds to ways in which the information collected about the customer will be used.

3.3. Web Site Related Factors

This group covers the factors that are typical for a web site. The Internet users' privacy perception depends on the web site that provides e-service. Therefore customer's interaction with the online company before, during and after the purchase needs to be considered. The factors reviewed in this group are: *familiarity with the online distributors' brand* (see: [6], [33]), *perceived benevolence* (see: [43]), *perceived credibility* (see: [40]), *perceived integrity* (see: [43]), *perceived risk* (see: [9], [15]), *services e-tailer's reputation* (see: [11], [37]), *web service quality* (see: [2], [18],[27].

Castañeda and Montoro [6] use the variable *familiarity* with the web site sponsor's brand as a determinant that influences customer's personal information disclosure and can also decrease customers' online privacy concerns. A lot of customers do not trust web sites that collect personal information about them, but differentiate between web sites that they are accustomed to and those unknown to them [33].

Perceived benevolence is the perception of how caring the web sites owner is and also how motivated to perform in the customer's best interest. *Perceived integrity* refers to the customer's perception of the degree of the web site's owner's honesty and consistency in fulfilling his obligations [43]. The web site reputation does not only have a major impact on customer's perception of trust but also reduces customers' privacy concerns [11].

The factor *perceived risk* includes two dimensions: (1) perceived Internet privacy risk and (2) Internet privacy concerns [9]. The *perceived Internet privacy risk* is the perceived overall risk of a company's behavior concerning the disclosure of the collected personal information on customers, including the selling or sharing that information with parties not directly involved in the transaction (like a third party, financial or government agencies). The dimension *Internet privacy concerns* refers to the perceived risk of opportunistic behavior of a particular company concerning the disclosure of a specific customer's personal information. Jih et al. [15] propose that the *perceived risk factor* implies the following: *time risk, functional risk, financial risk, social risk* and *physical risk*.

In their research of e-banking portals service quality Bauer et al. [2] take into consideration three service dimensions: *core service*, *additional service* and *problem solving service.* According to Khan and Mahapatra [18], service quality can be observed from two perspectives: the customer's perspective and the service provider's perspective. The customer distinguishes between two kinds of service quality: *sought quality* (service quality expected from the provider) and *perceived quality* (customers' overall impression of the service received from the provider). The service provider also differentiates between two kinds of service quality: *target quality* (the planned degree of service quality) and *delivered quality* (the realistic degree of the quality of the delivered service). The improvement of e-service quality is an important factor contributing to competitiveness on the online market [24].

3.4. Situational Factors

This group encompasses factors connected to a specific situation. An individual can react differently in the same online transaction scenario but under different situational conditions. While considering customers' online privacy perception, situational factors can not be neglected. Factors observed in this group are: *compensation for information provision* (see: [33]), *information congruency* (see: [22]), *information sensitivity* (see: [6], [22], [33]), *information type* (see: [3], [6], [21]).

Information congruency is the relevance of the collected information for the transaction context, wherein the impact of information congruency on privacy concerns depends on the sensitivity of the requested information (see: [41], [22]).

Information sensitivity refers to the degree of customer privacy concern regarding specific data in a specific situation, and can also be seen as the perceived level of information intimacy [22]. According to Castañeda and Montoro [6], information sensitivity 'enables privacy concerns to be compensated by requesting information that is relatively insensitive to being exchanged'. What the customer will perceive as sensitive will depend on the person and the situation. Therefore, it is necessary to define a clear boundary between the group of information that is personal for the customer and the one not personal for the customer [33]. The information about customers collected during their Internet transactions can be divided into three types: (1) anonymous information, (2) personally non-identifying information and (3) personally identifying information [8]. *Anonymous information* is the information about the customer's visit to a specific web site during which data, e.g. the customer's IP address, browser version and type, language and alike, are recorded. *Personally non-identifying information* is the information on the basis of which a customer can not be identified as an individual, such as the customer's age, gender, time of birth, occupation, education, interests and hobbies. *Personally identifying information* is the information on the basis of which a customer can be identified. This information includes the customer's first and last name, e-mail address, postal address, telephone number, credit card number and likewise. Berendt and Teltzrow [3] define three types of personal information that can be collected about an online customer: (1) user data; (2) usage data and (3) environment data–computer data. According to Sheehan and Hoy [33] 'compensation indicates an exchange of benefits from the situation'.

3.5. Legislation and Government Protection

This group of factors encompasses variables that are related to the legislation and government protection of customer privacy when using the Internet. Legislation protection concerning online privacy can be divided into two types: (1) protection used in USA and (2) protection used in Europe (see: [36], [1]). The observed factors are: *legislation and government protection* (see: [10], [29]), *privacy policy* (see: [10], [22], [33], [41]) and *regulating privacy* (see: [6], [22], [4151]).

From the customers' point of view these factors are very important because a web site does not only ask them to provide information but this information can also be manipulated by the web site. Policy (privacy policy/company policy) is the description of practices that a web site uses to handle customer information (collection, usage) [22]. Castañeda and Montoro [6] recommend that in *regulating privacy* laws promoting the opt-out option as part of web sites' control policy should be included. *Regulation* refers to self-imposed industry regulation and government-imposed regulation [41]. The customer has the right to be assured that online companies comply with privacy principles through external regulation or certification programs [32]. Berendt and Teltzrow [3] use the term *communication design* to describe the significance of the design and presentation of reasoning that is used to illustrate personal benefits to customers and *privacy policies* that a web site offers.

3.6. Online Privacy Consequences

To a considerable degree, Internet users' *online protecting behavior* is a consequence of their privacy perception. Online protecting behavior can be manifested in different forms, from refusing to do business with online firms, checking for cookies, to the removal of information from web sites [25]. The factors observed in this group are: *Internet trust* (see: [8], [9], [11], [21]), *perceived ease of use* (see: [19]), *perceived usefulness* (see: [19], [26]), and *personal Internet interest* (see: [9]).

According to Dinev and Hart [9], *Internet trust* reflects the confidence that customer personal information submitted over the Internet will be managed competently, reliably and safely, while *personal Internet interest* is the situation in which 'personal interest or cognitive attraction to Internet content override privacy concern'.

Lallmahammod [19] defines *perceived ease of usage* as the customers' belief that a specific technology usage will not require a huge effort, while *perceived usefulness* is defined as the customers' perception of the way in which technology usage will improve their performance. According to Lallmahammod, both perceived ease of usage and perceived usefulness are under the influence of perceived online security and privacy.

Customer trust in online transactions is important for the growth and development of e-commerce. Research results show that there is a great difference between the customer's privacy perception when they are online and when they are offline, even when doing business with the same company [8].

4. Research Model of Online Privacy

According to the Internet World Statistics [14], 23.8% of the world's population today uses the Internet. The widespread use of the World Wide Web as well as the customers' positive response to this kind of technology has opened the way to many types of business, among which online shopping and e-banking are the most widely used. However, there is no detailed information about the factors that influence online shopping or e-banking acceptance, nor about the factors that influence customer behaviour when using these e-services.

Therefore a research model of online privacy perceptions of e-banking/online shopping users is proposed. The proposed research model is illustrated in Figure 2. It proposes a relationship between Internet users' privacy perception and (1) customer – intrinsic factors, (2) customer and web site relationship, (3) web site characteristics, (4) situational factors and (5) legislation and government protection group of factors. For each group there are also illustrated constructs (scales) that are measured. By following the proposed categorization of factors that have influence over consumers' online privacy concerns, and an examination of the existing privacy literature a set of 94 items was collated. Items were created in three ways: (1) by using original items from previous work, (2) through modification of the original items, and (3) by creating new items.

Users' perception of the level of privacy protection when using e-banking/online shopping services was measured using a four-item scale. Scale was named *Users' privacy perception*. Users' privacy perception refers to users' evaluation and anxiety about how an online company or a bank will handle information that they collect about the users. Also, users' satisfaction with privacy protection during their online activity (everyday online activity), as well as satisfaction with privacy protection when using e-banking or online shopping services were measured (by using one item scale for each). *Users' satisfaction with privacy protection during their online activity (everyday online activity)* refers to the users' satisfaction with privacy practices (protection mechanisms) that an online service provider uses to secure users' online privacy. *Users' satisfaction with privacy protection when using e-banking or online shopping service* refers to the users' satisfaction with the ways in which an a bank or online company secure and protect users' online privacy. Items were based on the five-point Likert scale (for example '5'= strongly agree, '1'= strongly disagree).

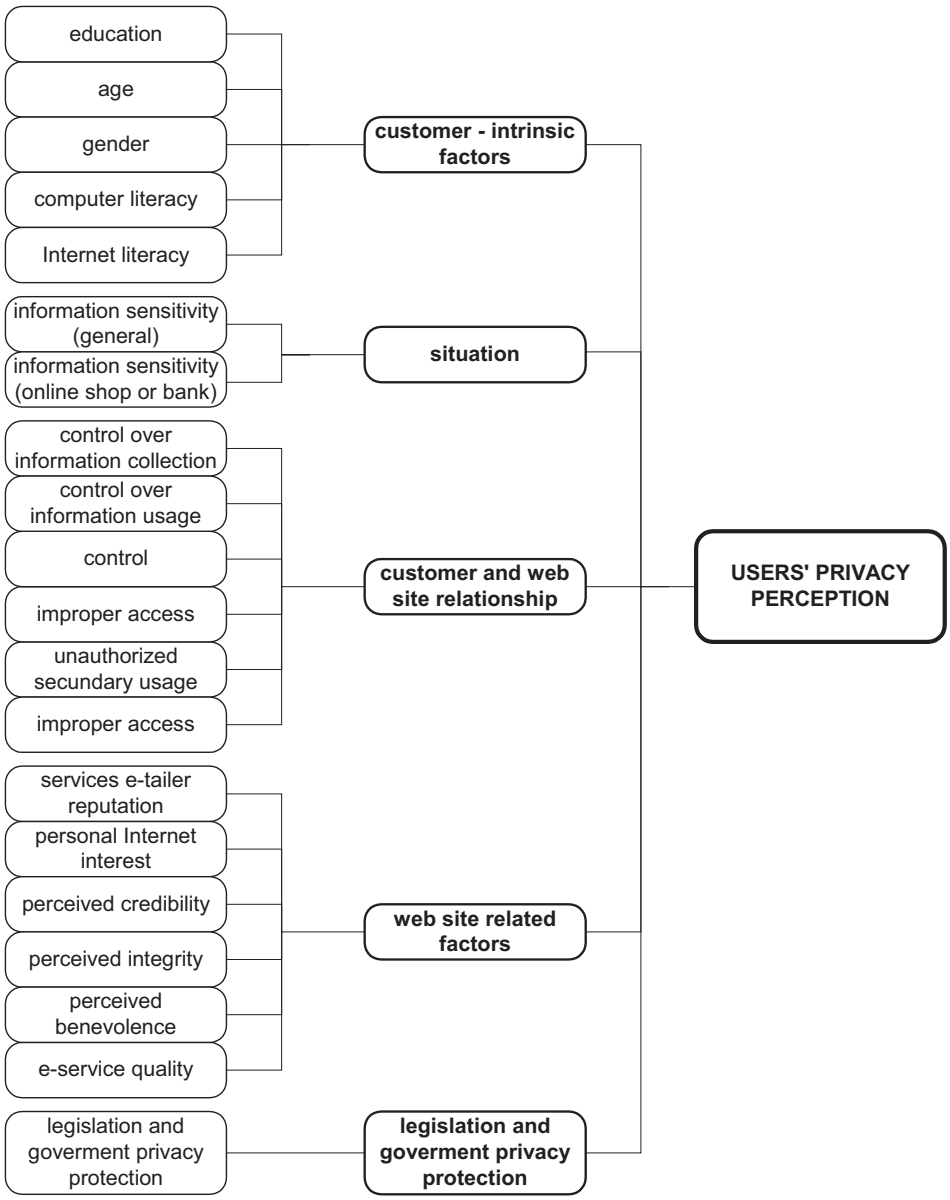

Figure 2. Research model of e-banking/online shopping users' privacy perception

Participants were individuals who had been using online shopping and e-banking service for at least a year. Data were collected using written and web-based questionnaires. In total 185 responses were collected. Of all the respondents, 116 (63%) were men and 69 (37%) were women. The average age of respondents was 33,2 years (ranged from 19 to 59).

Each construct (scale) was tested for internal consistency of the scale items with a reliability test. The reliability test was performed using Crombach's alpha coefficients. All the coefficients were above the proposed .70.

Results of the research indicate that consumers' satisfaction with general privacy protection when using online shopping or e-banking service is relatively high. Average score (mean) was 3,74, while customers' satisfaction with privacy protection during their everyday online activity was 3,49 (mean). Degree of users' privacy protection level when using online shopping/banking services was 3,39 (mean).

In order to explore the relationship between proposed factors (and specific constructs) that influence online privacy concerns, users' online privacy perception and satisfaction with online privacy protection, a correlation analysis was performed. Results of the correlation

analysis indicate that there is a significant positive relationship between users' privacy perception and constructs Control over information collection, Information sensitivity (general and in online shopping/e-banking context), Collection, Improper access, Perception of Internet privacy risk, and Legislation and government privacy perception (at level 0,01).

On the other hand, users' privacy perception does not correlate with satisfaction with the ways in which privacy is protected during their online activity (customers' satisfaction with privacy protection during their everyday online activity). Moreover, users' privacy perception does not correlate with satisfaction with the ways in which privacy is protected when using online shopping/e-banking services. In addition, demographic characteristics, computer and Internet usage or experience do not have influence on users' online privacy perception.

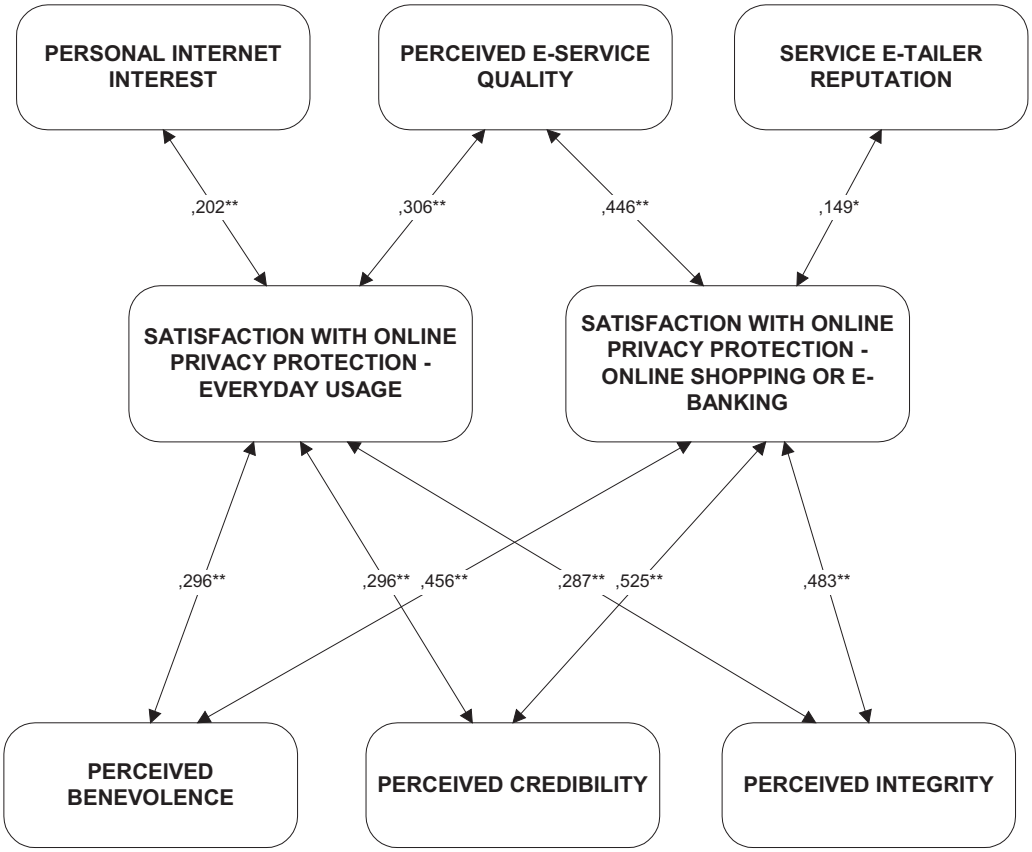

Figure 3. Correlation between factors that influence users' privacy perception and users' satisfaction with online privacy protection (*p<0,05, **p<0,01)

Figure 3. illustrates the correlation between satisfaction with online privacy protection (everyday usage and when using online shopping or e-banking service) and online privacy factors. Correlations are significant at the 0,01 level, apropos 0,05 level.

The way a user perceives e-service providers' (companies, banks, web portals) credibility, benevolence, integrity or the way he perceives the quality of delivered e-service depends on users' experience in present and past interactions with a specific service provider. Therefore, service providers must make an effort to deliver high quality service every time. Online companies must convince their users that they are honest and consistent in keeping their promises regarding price, delivery or customer service. Also, that they are capable to deliver what they had promised. The way a user will perceive e-service quality depends on his evaluation of his experience during the whole interaction with the service provider through a web site. This includes the process of searching and browsing for information about a service or a product, the ordering of a specific item, payment, delivery and eventually complaints. In

addition, users' evaluation of how easy it is to use a particular web site, navigability of the web site, aesthetics of the web design, and the content of the web site are also important. Content of the web site refers to usability, usefulness of content, adequacy of information and accessibility of content. On the other hand, a user will evaluate reliability, efficiency, support, communication, and security of every web page. Therefore, the customer must have the central place in online companies' strategies. All of the above-mentioned factors influence users' satisfaction with their online privacy protection. Also, satisfaction with online privacy protection has an impact on users' online behaviour. If online companies do not pay attention to these issues a consequence can be that customers will be more reluctant to disclose or to allow future use of their personal information. Furthermore, customers will avoid using Internet as a communication media.

5. Conclusion

Information is a significant resource in the present customer-supplier relationship. Companies use all possible ways to collect information about their customers in order to offer services or products that better meet their customers' needs and desires. Although new technologies offer increased capabilities of collection, storage, usage and dissemination of information, collecting and using customer information in a way that would make customers feel comfortable presents a challenge for companies. The information that is being collected in online transactions is not only related to the personal information of specific customers but also to information about their preferences in shopping, hobbies, and lifestyle. When customers become aware of all the possible consequences of information collection (and usage) about them, their privacy concern is likely to be raised.

Every day people can read in the newspapers or on Internet portals (or hear on TV) about new cases of data loss, situations where data were stolen or data were sold to the third party. People are becoming nervous and very careful about their personal information.

Privacy and fraud are viewed as main causes of the limited usage and expansion of e-commerce [17]. Privacy in online environment covers issues related to users' concerns for his personal information collection, storage, usage and dissemination. Fraud is one of possible consequences of improper handling of users' personal information and (some) companies aim to maximise their profit. Internet users' privacy concerns can be viewed through: (1) concern for personal information collection by a third party; (2) concern related to collected personal information storage/archiving; (3) concern for collected personal information collation and dissemination; (4) concern for decontextualization of the Internet users' personal information [12]. Results of the research presented in this article confirm this. According to the results users' online privacy perception is influenced by (1) users' perception of control over information collection during their everyday online activity, (2) type of information that are asked in order to perform a transaction, (3) concerns regarding improper access to information that were collected, (4) users' perception of information collection during their interaction with a bank or an online company through a web site, (5) users' perception of Internet privacy risk, (6) and perception of legislation and government privacy protection.

Online privacy protection should be the responsibility of all participants that are included in the online market. First of all, an individual must take responsibility for his information. He should value and protect his personal information. He must understand and make decisions about what information he should and shouldn't share. In addition, when entering an online transaction he must understand how and which information (about him) will be collected. An individual must obtain knowledge about the length of time the collected information will be kept, who will have access to them, for which purpose they will be used, and how will they be secured. Internet user should not be a passive participant in an online transaction, and shouldn't allow an online company to force him to share his personal information. User should actively protect his information (use all possible protection mechanisms) and ask/demand of the online company (or any organization that is participating in online market) to protect his online privacy.

Furthermore, online companies (organizations that offer their services or products online) should take responsibility for protecting and securing customers' online privacy. They should recognize that the customer's perceptions of privacy protection in actual interactions are of significant importance to customers when they decide to conduct business with a specific company in the future [10]. Therefore, they should inform customers about privacy practices that they use. Online companies should define their responsibilities and behaviour regarding protection of customer personal information. They should use all possible mechanisms to make clear to their customers that they will not misuse the collected information or sell it (like using a privacy seal, privacy policy). When developing a new information system an online company should pay attention to implement all customers' needs regarding protection of his personal information. Furthermore, study results that were presented could be used to improve new e-service development or a modification of present e-services. At the very beggining, when defining an e-service, online company should include these requirements (customers' requirements regarding their online privacy protection). First, the new e-service should include mechanisms that will give the customer control over his information collection. Online company should the ask customer's permission to collect information about him, and his activity on a specific (online company's) web site. Second, online company should protect the collected customer information from improper access. There are many new technology-based solutions regarding these issues. Online company should revise all possible solutions and incorporate them in access control. Accordingly, the customer should be informed. Finally, online company should regulate customer online privacy protection according to present privacy legislature.

On the other hand, online companies should continuously analyse all threats and risks in order to understand what needs to be protected and from whom (hackers, viruses) or from what (fire, earthquake, overflow, burglary).

Every government should uphold privacy protection of his citizens. Government should make an effort to ensure a market environment in which customers' and companies' needs will be balanced. Government should proclaim and invest in usage of all possible technologies in order to protect and secure citizens' personal information. On the other hand, all companies (organizations) that do not comply with data protection and data security rules should be punished. Goverment should make an effort to further develop supplementary and alternative measures (like Privacy Enhancing Technologies e.g. encryption, security breach notification) to protect invividuals' rights regarding their privacy.

In this article a systematization of attributes that influence the Internet users' privacy perception is proposed. The identified attributes are grouped into five groups: (1) customer-intrinsic factors, (2) customer and web site relationship, (3) web-site related factors, (4) situational factors, and (5) legislation and government protection.

Although the proposed systematization and grouping of factors that influence the Internet users' privacy perception may have limitations, the presented work can be used as an instrument for monitoring, measurement and comparison of the impact on the Internet users' privacy perception in empirical research and professional studies.

References

1. Ashwort, L; Free, C, Marketing dataveillance and digital privacy: using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, 67:107-123, 2006.
2. Bauer, H.H; Hammerschmidt, M; Falk, T. Measuring the quality of e-banking portals. *International Journal of Bank Marketing*, 23(2):153-175, 2005.
3. Berendt, B; Teltzrow, M. Addressing user's privacy concerns for improving personalization quality: towards an integration of user studies and algorithm evaluation. In *Intelligent Techniques for Web Personalization, IJCAI 2003 Workshop*, *ITWP 2003*, pages 69-88, Acapulco, Mexico, 2003.

4. Burgoon, J. Privacy and communication. In *Communication Yearbook 6*, pages 206-249, Beverly Hills, California, 1982.
5. Buchanan, T; Paine, C; Joinson, A.N; Reips, U-D. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2):157-165, 2007.
6. Castañeda, J.A; Montoro, F.J. The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research*, 7(2):117-141, 2007.
7. Castañeda, J.A; Montoso, F.J; Luque, T. The dimensionality of customer privacy concern on the internet. *Online Information Review*, 31(4): 420-439, 2007.
8. Chellappa, R.K. Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security. www.bus.emory.edu/ram/Papers/sec-priv.pdf, downloaded: December, 22nd 2009.
9. Dinev, T; Hart, P. An extended privacy calculus model for e-commerce transaction. *Information System Research*, 17(1):60-81, 2006.
10. Dolnicar, S; Jordan, Y. Protecting customer privacy in company's best interest. *Australasian Marketing Journal*, 14(1):39-61, 2006.
11. Eastlick, M.A; Lotz, S.L; Warrington, P. Understanding online B-to-C relationships: an integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8):877-886, 2006.
12. Goldie, J.L. Virtual communities and the social dimension of privacy. *University of Ottawa Law and Technology Journal*, 3(1):133-167, 2006.
13. Harkiolakis, N. A six-dimensional approach to online privacy, IBLT 2006–Copenhagen. http://harkiolakis.org/research/Privacy/A%20Six-Dimensional%20 Approach%20to%20Privacy.ppt, downloaded: December, 22nd 2009.
14. Internet World Stats, usage and population statistics, Internet usage statistics, http://www.internetworldstats.com/stats.htm, downloaded: December, 22nd 2009.
15. Jih, W-J; Wong, S-Y; Chang, T-B. Effects of perceived risks on adoption of Internet banking services: an empirical investigation in Taiwan. *International Journal of e-Business Research*, 1(1):70-88, 2005.
16. Joinson, A.N; Paine, C; Buchanan, T; Reips, U-D. Watching me, watching you: privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom. *Journal of Information Science*, 32(4):334-343, 2006.
17. Kalvenes, J; Basu, A. Design of robust business-to-business electronic marketplace with guaranteed privacy. *Management Science*, 52(11):1721-1736, 2006.
18. Khan, M.S; Mahapatra, S.S. Service quality evaluation in internet banking: an empirical study in India. *International Journal of Indian Culture and Business Management*, 2(1): 30-46, 2009.
19. Lallmahamood, M. An examination of individual's perceived security and privacy of the Internet in Malaysia and the influence of this on their intention to use e-commerce: using an extension of the technology acceptance model. *Journal of Internet Banking and Commerce*, 12(3), 2007.
20. LaRose, R; Rifon, N. Your privacy is assured – of being disturbed: websites with and without privacy seals. *New Media and Society*, 8(6):1009-1029, 2006.
21. Liu, C; Marchewka, J.T; Lu, J; Yu, C-S. Beyond concern: a privacy-trust-behavioral intention model of electronic commerce. *Information and Management*, 42(2):289-304; 2004.
22. Lwin, M; Wirtz, J; Williams, J.D. Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, 35(4):572-585; 2007.
23. Malhotra, N.K; Kim, S.S; Agarwal, J. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information System Research*, 15(4):336-355, 2004.
24. Mekovec, R; Bubaš, G; Vrček, N. A method for improvement of objectivity of e-service quality evaluation. *Journal of Information and Organizational Sciences*, 31(2):15-27, 2007.

25. Milne, G.R; Rohm, A.J; Bahl, S. Customers' protection of online privacy and identity. *The Journal of Customer Affairs*, Vol. 38, No. 2, 2004, pp. 217-232.
26. Milne, G.R; Rohm, A.J. Consumer privacy and name removal across direct marketing channels: exploring opt-in and opt-out alternatives. *Journal of Public Policy and Marketing*, 19(2):238-249, 2000.
27. Miranda, F.J; Cortés, R; Barriuso, C. Quantitative evaluation of e-banking web sites: an empirical study of Spanish banks. *The Electronic Journal Information Systems Evaluation,* 9(2):73-82, 2006.
28. Miyazaki, A.D; Fernandez, A. Consumer perception of privacy and security risks for online shopping. *The Journal of Consumer Affairs*, 35(1):27-44, 2001.
29. Molla, A; Licker, P.S. eCommerce adoption in developing countries: a model and instrument. *Information and Management*, 42(6):877-899, 2005.
30. O'Neil, D. Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review*, 19(1):17-31, 2001.
31. Paine, C; Reips, U-D; Stieger, S; Joinson, A; Buchanan, T. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, 65:526-536, 2007.
32. Schwaig, K.S; Kane, G.C; Storey, V.C. Compliance to the fair information practices: how are the Fortune 500 handling online privacy disclosures? *Information and Management*, 43(7):805-820, 2006.
33. Sheehan, K.B; Hoy, M.G. Dimensions on privacy concern among online consumers. *Journal of Public Policy and Marketing*, 19(1):62-73, 2000.
34. Smith, R; Shao, J. Privacy and e-commerce: a customer-centric perspective. *Electronic Commerce Research*, 7(2):89-116, 2007.
35. Spiekerman, S; Grossklags, J; Berent, B. Stated privacy preferences versus actual behavior in EC environments: a reality check. In *Proceedings der 5. Internationalen Tagung Wirtschaftsinformatik*, pages 129-148, Augsburg, Germany 2001.
36. Strauss, J; Rogerson, K.S. Policies for online privacy in United States and European Union. *Telematics and Informatics*, 19(2):173-192, 2002.
37. Teltzrow, M; Meyer, B; Lenz, H-J. Multi-channel customer perceptions. *Journal of Electronic Commerce Research*, 8(1):18-31, 2007.
38. Tufekci, Z. Can you see me now? Audience and disclosure regulation in online social network sites. *Bulleting of Science, Technology and Society*, 28(1):20-36, 2008.
39. Turow, J; Hennessy, M. Internet privacy and institutional trust: insights from a national survey. *New Media and Society*, 9(2):300-318, 2007.
40. Wang, Y-S; Wang, Y-M; Lin, H-H; Tang, T-I. Determinants of user acceptance of Internet banking: an empirical study. *International Journal of Service Industry Management*, 14(5):501-519, 2003.
41. Wirtz, J; Lwin, M.O; Williams, J.D. Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, 18(4):326-348, 2007.
42. Woo, J. The right not to be identified: privacy and anonymity in the interactive media environment. *New Media and Society*, 8(6):949-967, 2006.
43. Yousafzai, S.Y; Pallister, J.G; Foxall, G.R. A proposed model of e-trust for electronic banking. *Technovation*, 23(11):847-860, 2003.