8-7-2011

Differentiating Privacy and Security: A Content Analysis of B2C Websites

Marie Caroline Oetzel
Vienna University of Economics and Business, marie.oetzel@wu.ac.at

Barbara Krumay
Vienna University of Business and Economics, barbara.krumay@wu.ac.at

Differentiating Privacy and Security: A Content Analysis of B2C Websites

Marie Caroline Oetzel
Vienna University of Economics and Business
marie.oetzel@wu.ac.at

Barbara Krumay
Vienna University of Economics and Business
barbara.krumay@wu.ac.at

ABSTRACT

Privacy and security are important topics in research and business. This work on one hand offers a way to differentiate these two topics and provides information about different privacy regulations already existing in Europe and the US. We clarify definitions of information privacy and state that privacy and security are not the same, although most companies do not differentiate. A content analysis conducted in 2008 and 2011 of B2C-companies' websites is used to demonstrate how interweaved these two terms and the representation of terms and conditions (T&C) are presented. The data is analyzed in terms of numbers, how often links to the topics exist; positioning, where these links are located on the web pages; and identifiers, which represent the topics privacy, security, and T&C. Based on this information, the relation between privacy, security, and T&C is analyzed and interpreted.

Keywords

Privacy, security, privacy awareness, security awareness, B2C websites.

INTRODUCTION

"Security and privacy tend to be articulated at a level of abstraction that often makes their specific manifestations less than obvious, to either customers or system developers" (Shapiro, 2010). In this paper, we want to dig deeper into this phenomenon of information security and privacy not being clearly differentiated. The discipline of security already exists for some time in research as well as in practice. Information security management procedures and standards are available and widely accepted. Companies use security certifications that show compliance to the existing standards to promote their image and to gain customers' trust. On the other hand, the conceptual notion of privacy is not new either but practical procedures and standards that translate this concept into comprehensive and specific requirements for information systems do not exist yet. A clear differentiation of the terms and appropriate management procedures is important for both, companies and consumers. Companies need a clear differentiation in order to be able to identify and employ technical and organizational controls that address issues of both security and privacy. Consumers, on the other hand, might seek for a clear distinction due to the increasing awareness of privacy aspects. They want to be able to judge how the data processing companies treat their personal data.

Starting with a conceptual description of the status quo, we then describe the results of a content analysis of B2C websites. We want to demonstrate how companies use the terms security and privacy, how they differentiate the terms and how they communicate them to their customers on their websites.

DEFINING INFORMATION SECURITY AND INFORMATION PRIVACY

Information Security

The most common definition of information security, mostly referred to as security, is based on the well-known triad of confidentiality, integrity and availability (CIA). It is either formulated as an attempt to ensure these three requirements in computer systems (Pfleeger and Pfleeger, 2003) or more definite as their preservation (ISO, 2008). Peltier defines security without mentioning the triad but explains it in other words by saying: "Information security encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets" (Peltier, 2000). This triad is sometimes expanded with other requirements as in ISO/IEC 27002: "in

addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved" (ISO, 2008). Flavián and Guinalíu describe security as the "technical guarantees" that ensure that legal requirements and good practices are fulfilled (Flavián and Guinalíu, 2006).

These definitions of security have in common that they adopt a technical perspective. They are concerned with the development of measures to ensure confidentiality, integrity and availability of information in computer systems. The goal is to implement adequate functionality in computer systems to protect these systems and the data that is processed by them. This technical or functional perspective can easily be explained as most protagonists in this field stem from computer and information sciences.

Information Privacy

The first definition of privacy occurs in 1890, in the famous article "The Right to Privacy" of Warren and Brandeis, two American lawyers who saw the need to define this term in the light of the upcoming technology of photography and the publication of resulting photographs. They defined privacy as "the right to be let alone" (Warren and Brandeis, 1890).

The most common definition used today originates from Westin who defines privacy or more precisely information privacy as "the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" (Westin, 1967). Thus, he not only considers the individual but also expands the right of privacy to groups and institutions. Some scholars take the position that this definition goes not far enough and ask for "privacy zones" individuals can grant access to (Moor, 1997).

Nevertheless, Solove criticizes that existing definitions of privacy are "far too vague to guide adjudication and lawmaking" (Solove, 2006). He proposes a new framework that attempts to describe privacy problems in a comprehensive manner and aims at a more coherent understanding of the concept of privacy. He especially focuses on activities that cause privacy problems because "often, technology is involved in various privacy problems, as it facilitates the gathering, processing, and dissemination of information. Privacy problems, however, are caused not by technology alone, but primarily through activities of people, businesses, and the government. The way to address privacy problems is to regulate these activities" (Solove, 2006).

In contrast to the definitions of security, the definitions of privacy adopt a legal perspective. Privacy is defined as a legal right. The main focus lies in the control of information (e.g. personal, sensitive personal) and information flows as well as access restriction to this information. Similarly to the above-described technical perspective of security, the legal perspective of privacy can be explained as the protagonists of the field stem either from law or philosophy.

In the European community, the term data protection is often used instead of privacy. Especially federal and national laws mostly use the term data protection. Data protection is considered as the operationalization of privacy (Fischer-Hübner, 2001). This more practical perspective on privacy and the accompanying avoidance of philosophical discussions about privacy may explain the usage of the term data protection in the European community.

Information Privacy Concepts

Although the translation of abstract concepts like the security triad into comprehensive specific requirements for computer systems is complex and problematic, a large body of knowledge already exists in the computer science community (Shapiro, 2010). No such body of knowledge exists for information privacy concepts and in contrast to the security triad there are no commonly acknowledged concepts, yet. Thus, it is worthwhile to look at some privacy concepts that are accepted by large communities, such as the OECD, EU, or US.

The oldest and most broadly accepted description of privacy principles are the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980) from 1980. These guidelines differentiate between principles of national and international application. Principles of national application are: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness and individual participation. Principles of international application are free flow and legitimate restrictions. The goal was to harmonize national laws and to motivate member states to include a certain degree of privacy protection into their national laws.

The EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EC, 1995) was adopted in 1995. Its articles describe the following principles: data quality, legitimate processing of personal data, legitimate processing of personal sensitive data, the data subject's right to be informed, the data

subject's right of access to data, to correct and erase data, the data subject's right to object, confidentiality and security of processing and notification. The principles show that the EU Directive explicitly differentiates between personal data and sensitive personal data. This differentiation has been fairly new at this point in time and is not yet reflected in national laws. In contrast to the OECD guidelines, this EU Directive is binding and needs to be translated into national law by all member countries.

In the US, the Federal Trade Commission's Fair Information Practice Principles (FIPs) (FTC, 1998) are widely accepted concepts of privacy. The core principles are: notice/awareness, choice/consent, access/participation, integrity/security and enforcement/redress.

These perspectives on information privacy share the main ideas, e.g. principles of the OECD guideline have been incorporated into the EU Directive. Nevertheless, FIPs offers the fewest details and EU Directive offers the most details, which suggests that the latter might be most feasible to be taken as a basis in order to realize a translation of the abstract concepts into comprehensive specific requirements for computer systems and organizations.

The Relationship between Privacy and Security

The fact that all three guidelines described in the previous paragraph include security as a principle shows that both concepts are related. Two different relationships can be observed: first, all three guidelines, OECD, FIPs and EU Directive, consider security as one of the means, besides others, to guarantee privacy and thus establish a hierarchical relationship where privacy is located above security; third, existing security management standards like ISO/IEC 27002 (ISO, 2008) and the German Federal Office for Security in Information Technology's IT Baseline Protection Catalogs include privacy objectives in their compliance sections and thus establish a hierarchical relationship where security is located above privacy.

The latter relationship is supported by Kim and Ahn who define information privacy as being part of the construct of web security (Kim and Ahn, 2006) and Clarke who claims that companies acknowledge privacy to be a strategic variable and thus factor it into their security and risk management frameworks (Clarke, 2009). Bansal and Zahedi observed similar relationships and tried to solve this issue by defining dimensions that are either unique to the concepts of privacy and security or overlapping (Bansal and Zahedi, 2010). They also mention that privacy and security are either considered as being separate concepts or being the same, which supports our claim that there is not yet a clear distinction that is broadly accepted. Finally, Flavián and Guinalíu introduce another aspect when considering different perspectives. On the one hand, consumers do not differentiate between security and privacy, and on the other hand, companies and public institutions distinguish legal and technical aspects to adequately fulfill privacy and security requirements (Flavián and Guinalíu, 2006).

METHODOLOGICAL APPROACH

Content Analysis

Content analysis is a well-defined, structured approach, which consists of different steps, agreed upon by different experts (Mayring, 2003; Neuendorf, 2002). These steps include the development of a coding scheme based on a literature review (Belanger, Hiller and Smith, 2002; Cao, Zhang and Seydel, 2005; Udo, 2001). This coding scheme is used to sketch a coding sheet and a codebook, which includes detailed instructions what and how to code. A training-set on websites outside the Fortune top 500 (531 – 600) was used to evaluate the coding sheet. In this evaluation we recognized, that terms and conditions (T&C) is a concept closely related to security and privacy. Due to this fact, we decided to include links to T&C in our analysis.

The reliability of the instrument was measured by intracoder and intercoder reliability, using the Holsti method (Figure 1). The intracoder reliability measures the variation shown by one coder over time (Neuendorf, 2002). The coder codes the same website twice and the differences are calculated. The intracoder reliability was at the very high level of 0.99 – 1.00. To ensure the comparability between the two data sets, time-dependent intracoder reliability was measured in terms of recollecting data on the stored websites from 2008. The reliability in this setting is between 0.95 – 0.97, which is acceptable.

The intercoder reliability measures the agreement of coders, compared in pairs (Neuendorf, 2002). The coders are coding the same object (in this case: a website) and the varying factors are calculated. The measured intercoder reliability is in a range between 0.81 – 0.93, which is good. Five coders were trained and conducted the analysis. The training was done on companies' websites outside the Fortune top 500 (501 – 530).

$$PA_O = \frac{2A}{(n_A + n_B)}$$

PA_O = proportion agreement
$2A$ = agreements of two coders
n_A = number of units coded by coder A and B
n_B = number of units coded by coder A and B

Figure 1: Holsti-Formula (Neuendorf, 2002)

Data Collection and Data Set

The front page (FP) and the customer service area (CSA) of each website were investigated. Terms like support, help, customer service, FAQ, 'contact us' are indicators for a CSA. A strict ranking of what to target when investigating the CSA was given to the coders in the codebook. A web front-end was used as the representation of the final coding sheet. The collected information was stored in a database.

The sample holds 283 out of 500 companies, were 79 are pure B2C-companies and 204 are both, B2B and B2C (e.g. Petroleum Refining). The other websites within the Fortune Top 500 ranking were excluded, because they are either pure B2B (164) or governmental sites (37), were not accessible at the time of the content analysis (12) or in a language, not familiar to the coders (4). A comparison between the status of 2008 and 2011 is meant to show the changes within these years. The companies and websites to be investigated are based on the top 500 companies 2007, published by Fortune. The categorization of B2C-companies was done in 2008 and used in the 2011 evaluation again to investigate the same companies in both evaluations.

PRIVACY AWARENESS ON WEBSITES IN B2C – ANALYSIS AND RESULTS

We want to demonstrate how often privacy is stated on these websites in terms of a link on the front page (FP) or the customer service area page (CSA), where it is located on the page and if a difference concerning link and naming between privacy, security, and T&C exists. Furthermore we describe how specific industries and countries in the sample represent the evaluated terms. The data analysis was done in different steps. First, an overall analysis was done purely considering the occurrence of privacy, security and T&C on the front page and the CSA. Second, the positioning of the variables was investigated. Third, the identifiers of the three variables were analyzed.

Overall Analysis

Table 1 presents detailed results; some outstanding results are discussed here. Out of the 283 companies investigated, 242 in 2011 (2008: 220) have links representing privacy on their front page and 237 (2008: 237) have links representing T&C on the front page. Security is not represented that often, only 115 times on the front page in 2011 (2008: 73). Privacy and security coincide with each other in 110 cases (2011), privacy and T&C in 213 times (2011).

	2008		2011	
	Front page	CSA	Front page	CSA
Represent all three links (privacy, security, T&C)	58	53	98	96
Privacy	220	140	242	219
Security	73	64	115	112
T&C	237	145	237	219
Privacy and security	65	57	110	107
Privacy and T&C	195	124	213	196

Security and T&C	65	59	102	100
Privacy and security without T&C	7	1	10	6
Privacy and T&C without security	137	69	113	98
Security and T&C without privacy	7	2	4	4

Table 1: Connection of Representation of Links

When comparing FP and CSA, 195 times there is no difference, 93 times the security representation is the same on both pages. 196 times the T&C are the same on both investigated pages.

This clearly demonstrates that a definite distinction between the three main terms investigated is not represented in the data set.

Analysis of Positioning

Besides the pure analysis of the existence of representations of privacy, security, and T&C, the position of the link on the web page was recorded. This is important due to the way users approach websites and relevant in terms of first-glance-impression influencing the perception and attitude of the customer towards a web page (Tsygankov, 2004). The most important positions are center, top and left side of a web page. Bottom and right side are not recognized by the user on a first glance (Gullikson, Blades, Bragdon, McKibbon, Sparling and Toms, 1999; Pan, Hembrooke, Gay, Granka, Feusner and Newman, 2004).

On the front page, most of the links are located in the bottom line (footer) of the web page. 233 of the privacy links are in the bottom line (2008: 204) and only 8 are located at the top of the page. On the CSA, some links are located in the center, but not more than 6 in 2011. In 2008, privacy was located 18 times in the center. In 2011, in 90 cases all investigated links exist and are located in the bottom line. Concerning the position at the web page, 204 times privacy was equal to T&C. Detailed information about positioning on the web pages is given in Table 2.

	2008					2011				
	Center	Top	Bottom	Left	Right	Center	Top	Bottom	Left	Right
FP - privacy	2	7	204	5	1	0	8	233	1	0
CSA - privacy	18	3	108	10	0	5	7	195	15	0
FP - security	2	5	56	6	4	1	5	105	3	1
CSA - security	16	2	34	10	1	5	4	89	14	0
FP – T&C	2	9	216	2	2	0	6	229	2	0
CSA – T&C	9	5	123	7	1	6	4	199	10	0

Table 2: Positioning of Representations of Links

Concluding the positioning section, it is striking that the bottom line is predominant, although this is not a very prominent place to get attention of website users. On the other hand, this homogeneity is an advantage as users might get used to search for privacy, security and T&C in the bottom line (Nielsen, 2000).

Analysis of Identifiers

An important analysis has to be done in investigating the identifiers. First, an overall picture on identifiers is drawn and afterwards a sort method is used to categorize identifiers. Interestingly, some identifiers are used to represent the same content. Even more, in 2011 one identifier for all three categories was used 31 times on the front page, even 32 times on

CSA. The high coincidence of privacy and security identifiers on the front page (62) and CSA (59) is a hint that no clear differentiation exists (Table 3).

	2008		2011	
	Front page	CSA	Front page	CSA
All terms are equal	17	6	31	32
Privacy equals security	23	28	62	59
Privacy equals T&C	17	6	31	32
Security equals T&C	4	2	19	20

Table 3: Identifiers' Similarity

Besides the similarity of the identifiers, the identifiers hold terms, clearly connected to other categories. While the privacy identifier holds security 20 times (2011, FP), privacy was part of the security identifiers in 52 cases (2011, FP).

Some identifiers are more likely to be used than others. We present the 5 most mentioned identifiers of all categories. Concerning privacy, the most popular identifier is "Privacy Policy" (80 in 2008 and 90 in 2011) and "Privacy" without any additional information.

Identifier	2008	2011
Privacy Policy	80	90
Privacy	44	46
Privacy Statement	19	19
Privacy [& / and / +] Security	17	12
Datenschutz (Data Protection)	5	7

Table 4: Identifiers of Privacy (Top 5), FP

As already mentioned, privacy is highly represented in security identifiers. Due to this, the most used identifier is "Privacy & Security". Eye-catching is the prominent position of "Privacy Policy" (14 times) and "Privacy" (10 times) in the security identifiers in 2011 (Table 5).

Identifier	2008	2011
Privacy & Security	12	16
Privacy Policy	2	14
Security	12	13
Privacy	0	10
Privacy Statement	2	5

Table 5: Identifiers of Security (Top 5), FP

A more consistent picture is given when looking at the T&C identifiers (Table 6). The five identifiers with the highest appearance are holding terms like "legal", "Terms of use" or "conditions". "Terms of use" was found 58 times (2011) in the sample set, and "Legal Notice(s)" 29 times (2011).

Identifier	2008	2011
Terms of Use	53	58
Legal Notice	19	29
Terms & Conditions	22	29
Legal	30	28
Disclaimer	15	16

Table 6: Identifiers of T&C (Top 5), FP

The categorization of identifiers is based on card sort method (Lewis and Hepburn, 2010), which is used to group terms and find out similarities and differences. Unique statements were written on cards and grouped according to different ideas (Bernard and Ryan, 2009). Because this investigation was done to see how different privacy and security are represented on websites, three independent judges were asked to sort the statements as purely privacy related, privacy and security related, and T&C related. Afterwards they had to sort them according to their strength – the strongest statement of a group on top. The result of this sort method shows a clear picture. For privacy identifiers holding "privacy" plus a description (statement, policy, notice and the like) or privacy alone are seen as strong. Mixed identifiers – privacy together with the terms "security" or "legal" are seen as medium explaining. Weak identifiers are all those that do not contain the word privacy. Almost the same picture is given for security concerning strong and weak identifiers. Medium explaining security identifiers are similar to the medium explaining privacy identifiers but contain the additional term "security certificates". Concerning T&C, the judges found no medium explaining identifiers just weak and strong ones. Almost all identifiers are seen as strong, except identifiers having exclusively "privacy" or "security" in the naming (Figure 2).

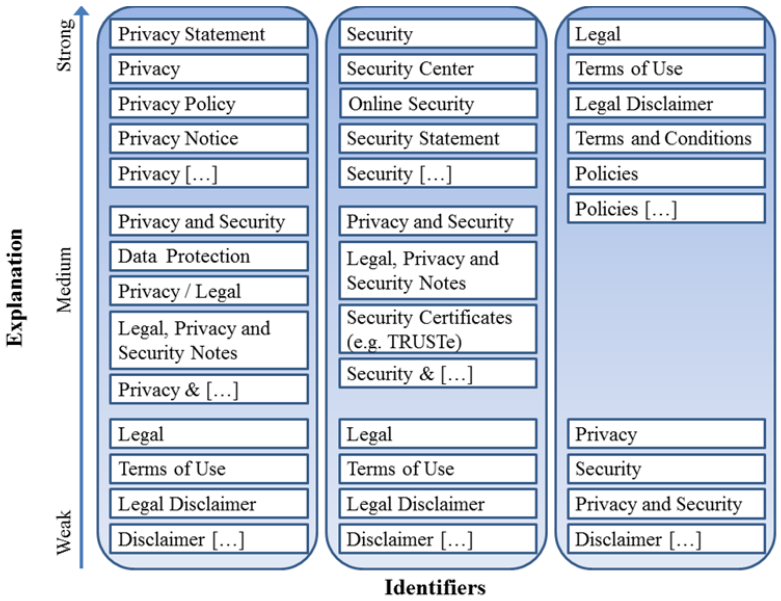

Figure 2: Categorization of Identifiers

Analysis by Country

Most companies in the sample set are either located in the US, Great Britain, Germany or Japan. Privacy seems to be an important issue in the US, where 95.92 % of the web pages investigated offer a privacy link on the front page. In Great

Britain (25 out of 27), Japan (21 out of 24) and Germany (26 out of 28) it is highly represented, too. This awareness is not given for security: US (59), Britain (12), Germany (6) and Japan (4). A slight increase since 2008 is recognizable in security representations. The highest representation of security is given in Canada (7 out of 8), showing in additions 8 out of 8 results in privacy. T&C are almost as represented as privacy: Britain (24), Germany (24), Japan (21), US (83). Figure 3 shows an accumulated view of identifiers by regions.

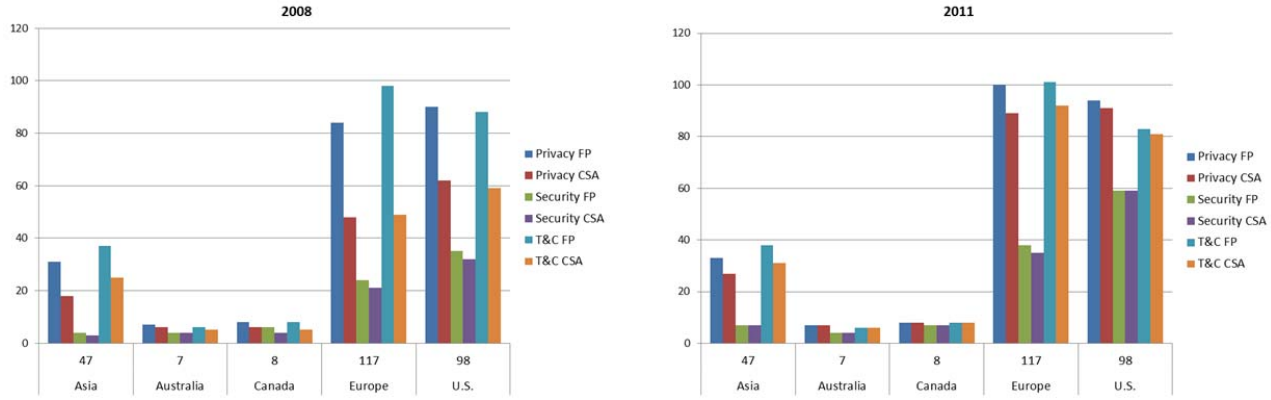

Figure 3: Representation of Identifiers in Different Regions

Analysis by Industry

Some industries are more likely to be privacy aware than others. In the investigated cases, we found that 44 out of 53 Banks (Commercial and Savings), Insurances (24 out of 26 – cumulated), Motor Vehicles (22 out of 25) and Telecommunications (14 out of 17), Pharmaceuticals (10 out of 11) are remarkable industries. Interestingly, only 16 out of 22 Petroleum Refining companies with B2C relations offer a privacy link on their website.

Changes from 2008 to 2011

132 companies still have the same identifiers for privacy on their front page in use as they had in 2008, 71 use the same in the CSA. For security, it is only 22 on the front page and 16 at CSA. T&C are still named the same way in 137 cases on the front page and in 69 cases at CSA. In the time-gap of three years the number of privacy statements increased (220 to 242) as well as the number of websites offering all three categories (privacy, security, T&C) from 58 to 98. Privacy is becoming a more independent topic, whereas security vanishes into privacy and T&C. The diversity in positioning disappeared and bottom line links of the investigated terms became more dominant. A shift in identifiers is given. In 2008, only 17 times one term was used to indicate all three targets, in 2011 we have this pictures 31 times. Privacy and security are named with the same term 62 times in 2011 (23 in 2008). The tendency in the data set is going towards more privacy, less security and more T&C on websites.

CONCLUSION AND FURTHER RESEARCH

The results of the content analysis support the claim of the conceptual reflections that privacy and security are not clearly differentiated and that privacy is gaining more importance. The lack of differentiation of the terms is supported by the observation that identifiers that represent the same content have increased between 2008 and 2011, thus increasing the dilemma and not clarifying it. Furthermore, the results show that the hierarchical relationship where security is located above privacy is represented clearly more often than the hierarchical relationship where privacy is located above security. This again supports the differentiation issue and it might support our claim that security management procedures, which include some singular privacy objectives, are already more broadly accepted than pure privacy management procedures. Finally, the categorization of identifiers, where a mix of the terms is judged as being medium explaining whereas a clear distinction of

terms is judged as being strong explaining, shows that the existing confusion of terms is not helpful and a clear differentiation is needed. This finding also questions one of the perspectives of Flavián and Guinalíu , which expresses that consumers do not and do not want to differentiate the terms (Flavián and Guinalíu, 2006). The growing importance of privacy is observable based on the dominance of the term on the front page as well as its increased appearance between 2008 and 2011. The concluding country and industry perspectives also show a clear dominance of the term privacy.

As this analysis is restricted to the representational layer of companies i.e. their websites, it is not possible to draw a conclusion on how these companies operationalized privacy and security in their internal processes and procedures. Another question that remains is why companies still hide especially privacy related information in the bottom line of their website and do not use it as a strategic variable.

Further research must be done in terms of investigating how companies deal with this problematic phenomenon of security and privacy not being clearly differentiated. The analysis of different cultural perspectives onto this differentiation issue could also be beneficial. Another topic is how companies realize and integrate existing and upcoming standardized security and privacy risk managements and utilize these to generate benefits, e.g. customer trust.

REFERENCES

1. Bansal, G., and Zahedi, F. (Year) Trading Trust for Discount: Does Frugality Moderate the Impact of Privacy and Security Concerns?, in *Proceedings of the AMCIS 2010*, 2010.
2. Belanger, F., Hiller, J. S., and Smith, W. J. (2002) Trustworthiness in electronic commerce: the role of privacy, security, and site attributes, *The Journal of Strategic Information Systems* 11, 3-4, 245-270.
3. Bernard, H. R., and Ryan, G. W. (2009) Analyzing qualitative data: Systematic approaches, Sage Publications, Inc, 2009.
4. Cao, M., Zhang, Q., and Seydel, J. (2005) B2C e-commerce web site quality: an empirical examination, *Industrial Management & Data Systems* 105, 5, 645-661.
5. Clarke, R. (2009) Privacy impact assessment: Its origins and development, *Computer Law & Security Review* 25, 2, 123-135.
6. European Parliament and Council of the European Union (EC) (1995) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, 31-50.
7. Fischer-Hübner, S. (2001) IT-security and privacy: design and use of privacy-enhancing security mechanisms Springer Verlag, Berlin Heidelberg.
8. Flavián, C., and Guinalíu, M. (2006) Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site, *Industrial Management & Data Systems* 106, 5, 601-620.
9. Federal Trade Commission (FTC) (1998) Fair Information Practice Principles.
10. Gullikson, S., Blades, R., Bragdon, M., McKibbon, S., Sparling, M., and Toms, E. G. (1999) The impact of information architecture on academic web site usability, *Electronic Library, The* 17, 5, 293-304.
11. International Organization for Standardization (ISO) (2008) ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management.
12. Kim, M.-S., and Ahn, J.-H. (2006) Comparison of Trust Sources of an Online Market-Maker in the E-Marketplace: Buyer's and Seller's Perspectives, *The Journal of Computer Information Systems* 47, 1, 84-94.
13. Lewis, K. M., and Hepburn, P. (2010) Open card sorting and factor analysis: a usability case study, *The Electronic Library* 28, 3, 401-416.
14. Mayring, P. (2003) Qualitative Inhaltsanalyse Grundlagen und Techniken Beltz Verlag, Weinheim und Basel.
15. Moor, J. H. (1997) Towards a theory of privacy in the information age, *Computers and Society* 27, 3, 27-32.
16. Neuendorf, K. A. (2002) The Content Analysis Guidebook Sage Publications Inc., Thousand Oaks, California.
17. Nielsen, J. (2000) Designing web usability - the practice of simplicity, (7 ed.) New Riders Publications, Indianapolis.
18. Organisation for Economic Cooperation and Development (OECD) (1980) Guidelines on the protection of privacy and transborder flows of personal data.

19. Pan, B., Hembrooke, H. A., Gay, G. K., Granka, L. A., Feusner, M. K., and Newman, J. K. (Year) The determinants of web page viewing behavior: an eye-tracking study, in *Proceedings of the 2004 symposium on Eye tracking research & applications*, 2004, San Antonio, TX, 147-154.
20. Peltier, T. R. (2000) Information security risk analysis CRC press, Boka Raton, FL.
21. Pfleeger, C. P., and Pfleeger, S. L. (2003) Security in computing Prentice Hall PTR, Upper Saddle River, New Jersey.
22. Shapiro, S. S. (2010) Privacy by design: moving from art to practice, *Communications of the ACM* 53, 6, 27-29.
23. Solove, D. J. (2006) A Taxonomy of Privacy, *University of Pennsylvania Law Review* 154, 3, 477-560.
24. Tsygankov, V. A. (Year) Evaluation of website trustworthiness from customer perspective, a framework., in *Proceedings of the ICEC '04: 6th international conference on Electronic commerce*, 2004, 265–271.
25. Udo, G. J. (2001) Privacy and security concerns as major barriers for e-commerce: a survey study, *Information Management & Computer Security* 9, 4, 165-174.
26. Warren, S. D., and Brandeis, L. D. (1890) The Right to Privacy, *Harvard Law Review* 4, 5, 193-220.
27. Westin, A. F. (1967) Privacy and freedom London.