Marketing Implications of Information Society Privacy Concerns

Gheorghe ORZAN[1]
Călin VEGHEŞ[2]
Cătălin SILVESTRU[3]
Mihai ORZAN[4]
Ramona BERE[5]

Abstract

Privacy has become over the last decade one of the foremost social concerns, since the arrival of cheap and ubiquitous surveillance of both online and offline behavior. The Internet has facilitated access to intimate user knowledge for both official and private agents and most of modern marketing strategies are based on a wealth of personal user data used to target its specific needs and expectations, a process that has its obvious pros and cons, which have been heavily debated intensively in both academic and social venues. Our paper attempts to uncover some of the most important privacy-related aspects of modern consumers, with a focus on their preferences for information access, marketing messages exposure, attitudes towards disclosing, capturing, processing and employment of their personal data, as well as their attitude towards various forms of media associated with our modern Information Society.

Keywords: *marketing strategy, privacy, ICT, interactive marketing, social media*

JEL classification: P2, P210, O52

Introduction

The knowledge about the characteristics of women business - leaders and In the digital economy, information plays a key role, as currency that makes the knowledge society further develop. In such world, ensuring privacy of personal data without restricting data flows and the economic and social benefits generated can prove in practice to be quite challenging.

While we are aware that privacy implies more than information management, "information control (that is, data) is a leading conception of privacy in the age of the internet and world wide web" (Allen, 2005), in terms of privacy, from the perspective of information flows, we are aware of core principles that should be taken into consideration in view of ensuring the fine line between privacy and freedom of expression is set reasonably, so as not to limit each other. These principles include: awareness, choice / consent, access / participation and integrity / security (Internet Society, 2012). In terms of ensuring **awareness** with

[1] The Bucharest University of Economic Studies, Romania, Email: orzang@ase.ro
[2] The Bucharest University of Economic Studies, Romania, Email: c_veghes@yahoo.com
[3] The Bucharest University of Economic Studies, Romania, Email: mihai.orzan@ase.ro
[4] The Bucharest University of Economic Studies, Romania, Email: catalin@ase.ro
[5] The Bucharest University of Economic Studies, Romania, Email: ramona.bere@gmail.com

regard to collecting data, in view of protecting personal information, users should be informed with regard to the practices used by the entity for processing information before any personal information is collected from them. Requesting **consent** from user, allowing the user to choose whether their personal information is collected and with regard to its possible uses takes two forms: opt-in, choosing before data is collected and opt-out, choosing to exclude user data from database after being collected. Users should also have **access** to their personal data, and contest or contribute to ensure accurate and complete data. Finally, **security** of personal data should be provided, by setting appropriate means to enforce privacy standards through courts of meaningful informal, self-regulatory mechanisms (Winer, 2009).

These principles have been taken into consideration in designing the questionnaire used in the survey conducted in Romania in 2011 with regard to the Romanian consumer and direct marketing. The survey was conducted online, with focus on the attitude of consumers in relation to tools and techniques for direct communication in marketing. It was conducted by the staff of the Direct Marketing Strategies course, from the Faculty of Marketing within the Academy for Economic Studies, Bucharest. 153 persons provided answers to the questionnaire. In addition, the analysis takes into account information related to techniques used in the WorldWideWeb, whether in terms of techniques (cookies) used in developing websites for collecting and processing user / consumer information, or in terms of technological developments resulted from cloud-computing.

Thus, we analyze and debate on aspects related to direct marketing techniques and privacy issues, in a consumer-oriented approach, focusing on behavior of the Romanian consumer, with taking into consideration the fast development and use of ICT in business and the increasing regulations for ensuring consumer privacy.

1. Why interest in online?

In terms of preferred information sources about products and / or services, Romanian respondents highlighted electronic means as most preferred source of information, with the internet (32%) and e-mail (24.4%), followed by the television (11.6%) and mobile phone (7.3%), as presented in figure 1.

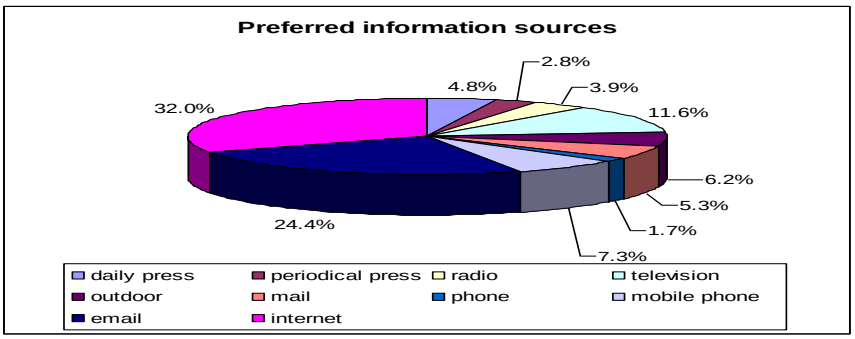

Figure 1. Preferred sources of information

Over 73% of respondents also indicated that protection of personal data is very important and 18.3% consider is as important.

Table 1. Importance of personal data protection

	Frequency	Percent
Very important	112	73.2
Important	28	18.3
Average importance	10	6.5
Less important	1	0.7
Not important	2	1.3
Total	153	100.0

While admitting that the means used in data collection (online) may have biased the results, such results prompted more interest in analyzing privacy issues in direct marketing in relation to the online environment. And even though such results regarding need for privacy are not unexpected, we consider of interest several aspects related to privacy, and raise into discussion aspects related to consumer behavior in function of means used in marketing, from the perspective of ensuring privacy of consumers' personal data.

2. Privacy and information control

Taking into consideration Allen's classification for privacy, based on concepts, values and phenomena most commonly discussed for it, in terms of (1) freedom of government or other outside interference with personal life – decisional privacy, (2) seclusion, solitude and bodily integrity – physical privacy, (3) confidentiality, anonymity, data protection and secrecy of facts about persons – informational privacy and (4) limits on the use of a person's name, likeness, identity, and other attributes of identity and exclusive possession – proprietary privacy (Allen, 2005), we have agreed to focus more on informational privacy.

The issues related to ensuring privacy of personal data starts from agreeing what represents personal data that should be protected. Just as there is no generally agreed upon definition of the concept of privacy, the results of our survey highlighted this aspect in terms of data perceived as personal data that should be protected by Romanian consumers, as pointed out below.

Table 2. Personal data that should be protected

Personal data	Percent	Personal data	Percent
Name	63.4%	Political preferences or orientations	32.7%
Gender	21.6%	Religious preferences or orientations	30.7%
Age	28.8%	Sexual preferences or orientations	34.0%
Profession	45.8%	Websites surfed	48.4%
Occupation	45.8%	Electronic mail content	62.1%
Working place	64.1%	Household goods	43.1%

Level of education	20.9%	Household access to services	30.1%
Level of income	75.2%	Hobbies	15.7%
Personal/family wealth	76.5%	Personal identification number	90.8%
Address	71.2%	ID series and number	92.2%
Phone	66.0%	Health	43.8%
Mobile phone	84.3%	Legal personal status	46.4%
E-mail address	61.4%	Biometric data	65.4%
Personal website	32.7%		

Respondents indicate a relatively high level of awareness in relation to their privacy-related rights, as illustrated in the table below, with lower level of awareness related to the right not to be subject to individual decisions regarding personal data, while in the case of the right to be informed about processing of personal data holds the highest level of awareness among respondents, of 94.8%.

Table 3. Level of awareness in relation to privacy related rights

Privacy-related rights	Percent
Right to have access to own personal data	77.1 %
Right to be informed about processing of personal data	94.8 %
Right to intervene on personal data	69.3 %
Right not to be subject to individual decision regarding personal data	40.5 %
Right to justice in any matter regarding personal data	81.7 %
Right to oppose to processing of personal data	84.3 %

As the perception of privacy is rather blurry, one solution was to define personal data in legislation as "any information referring to an identified or identifiable person; an identifiable person is a person that can be identified, directly or indirectly, particularly with reference to an identification number or to one or more specific factors of his physical, physiological, psychological, economic, cultural or social identity"[6].

[6] Art. 3 from Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, with modifications and amendments.

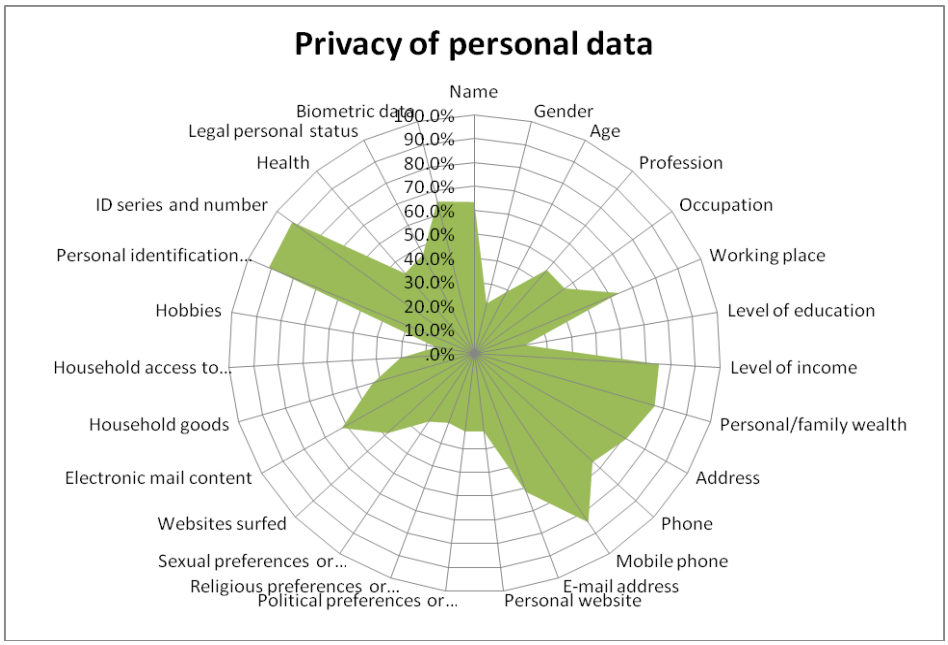

Figure 2. Privacy of personal data

In terms of interest in getting information about products or services that one wants to purchase, we could notice that preference is towards less invasive means of advertising / marketing, with 51.6% of respondents indicating that they would rather search information than receive it without having it requested it and 44.4% of respondents favoring both searching and receiving information.

Table 4. Preference towards receiving advertisements

	Frequency	Percent
Prefers to search	79	51.6
Prefers to receive	5	3.3
Prefers both	68	44.4
Does not know / does not answer	1	0.7
Total	153	100.0

Regarding interest in searching for commercial information or receiving it via e-mail or via social network account, one could notice that e-mail is the preferred contact medium, while in the case of social networks, more users prefer to search themselves for relevant offers, rather than to receive it for companies or third parties, as illustrated in Figure 3.

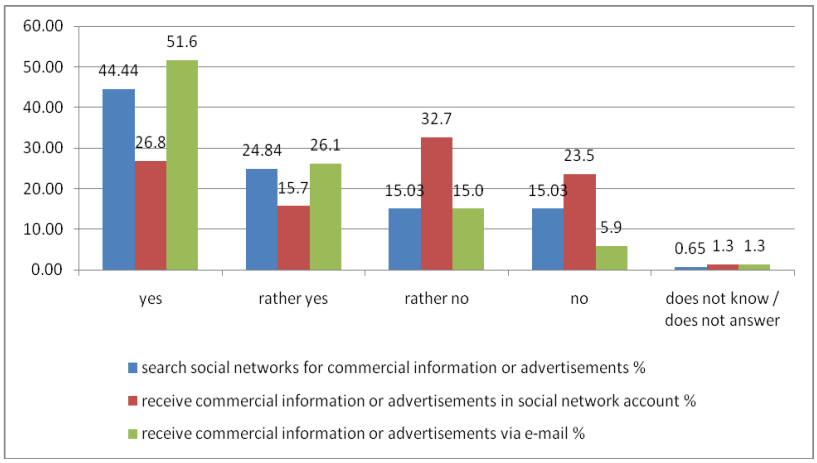

Figure 3. Online attitude towards commercial information

Direct contact with consumers, via mobile phone or phone, is perceived as more aggressive in direct marketing than usage of electronic means, as illustrated below.

Nevertheless, although not perceived as aggressive, the online environment enables tracking of the user's personal data, which in time may change the attitude of the Romanian consumer in relation to direct marketing online and to the level of privacy available online.

Table 5. Perceived levels of aggressiveness in direct marketing channels of communication

Level of aggressiveness	Mail	Phone	Mobile phone	Telematics	Internet
Aggressive	5.2	51.0	47.7	6.5	3.9
Rather aggressive	13.7	35.3	34.6	20.9	5.2
Rather non-aggressive	31.4	5.9	9.2	37.3	23.5
Non-aggressive	45.8	4.6	4.6	25.5	66.0
Does not know	3.9	3.3	3.9	9.8	1.3

Respondents perceive strongest the risk of abuses from various private companies, institutions or entities in cases of lack of personal data, 90.2% of the respondents indicating the private sector as more prone to abuses than the public one, with 60.1%. The risk of fraud is also perceived rather strongly, as second highest risk, in relation to various providers of goods and services. The least perceived risk is that related to limiting one's private space in relation with the other member of the community.

Table 6. Major risks faced in cases of lack of protection of personal data

Risks	Percent
Abuses from various private companies, institutions or entities	90.2%

Abuses from various public institutions or entities	60.1%
Exposing one's private to the other members of the community	65.4%
Submitting you to fraud as consumer by various providers of goods and services	83.0%
Limiting one's private space in relations with the other members of the community	45.1%

As pointed out in a report from a roundtable organized by the Internet Society at the WSIS Forum on 16 May 2012 at Geneva, Switzerland, titled "Data Privacy On A Global Scale: Keeping Pace With An Evolving Environment", the environment, including the online environment, in which our traditional privacy principles have to function, has to take into account significant changes in (Internet Society, 2012):

- the *volume of personal data* being collected, used and stored;
- the *range of analytics* enabled by personal data, providing insights into individual's movements, interests, and activities;
- the *value of the societal and economic benefits* enabled by new technologies and responsible data use;
- the *global availability* of personal data, supported by communications networks that enable continuous, multipoint data flows;
- and the *extent of threats* to privacy in such an environment.

Further on, we shall focus on the possible threats to privacy in the online environment, with reference to threats included in the websites, such as cookies, and also in cloud computing, used in collecting and processing of personal data. As the risk of limiting private space in relation with other members of the community is not perceived as strongly, in the context of the online environment we shall not analyze the threats to privacy that exist within social networks.

3. Online threats to privacy

Awareness-related. Although users should be informed with regard to practices used for processing information, in practice users are not always aware of the implications of such practices. Information is collected from users as they navigate the internet (Pope & Lowen, 2009). When online, the user provides information to others at almost every step of the way. Often this information is like a puzzle that needs to be connected before your picture is revealed. Information provided to one person or company may not make sense unless it is combined with information provided to another person or company.

Consent-related. Despite the fact that users should be requested to give their consent in the processing of their personal data, allowing the user to choose whether their personal information is collected and with regard to its possible uses, either as opting-in or as opting out, aspects related to consent are often misused (Veghes, et al, 2010).

In our survey, 53.3% of the respondents expressed their preference for opting-in, 42.5% for opting-out, and 5.2% for both options. In the case of opting-

in, that is, making a choice about personal data processing before the data is collected, users end up with personal data included in a database for a primary goal, for which they agree to provide their personal data, while later on, the data in the database may be used for secondary goals, some of them marketing-related, due to changes in circumstances. In addition, logging in various websites may require accepting a series of terms and conditions, which may be subject to change even without informing the user and requesting consent after changes have been made. Spamming is a result of such endeavors, with personal contact data included in a database being obtained and used to send unsolicited commercial information. As result, the need for creating user notification rules in case of data leaks and data breaches emerges, not only in the case of private companies but also in the case of public and government sector.

As mentioned in the 2011 ENISA (European Network and Information Security Agency) country report (2011, p.21), some ISPs have included an explicit spam policy in their terms and conditions, reserving the right to suspend user access for an unlimited period of time in the case of spam-related abuses are noted. In addition, anti-spam and / or antispyware are included by several Romanian ISPs in the internet protection packages provided to their clients, with such solutions being developed together with software producers.

Security related. Cookies can be used also for malicious purposes. They can be employed by nefarious agents to get information about a particular user's browsing history, his favorite websites, even his passwords and credit card information (Gurau, 2008). Even more, more recently cookies have been employed to track users over a series of websites, reporting on his entire online behavior and have been associated with other forms of privacy attacks, specifically phishing and distributed denial of service.

One of the latest additions of the online environment, **cloud services**, is already plagued by a series of privacy concerns of users, which concede that cloud stored data might be viewed by other parties, such as hackers, cloud storage providers, or law enforcement agencies (Ion, I., Sachdeva, N., Kumaraguru, P. and Capkun, S., 2011). As for e-mails and other forms of online storage, data saved online is not legally the property of the account users and as such, especially in countries such as US, this data can be searched and analyzed for various marketing objectives and later used to target its users for direct campaigns or, even more serious, sensible data stored online, such as credit card numbers and personal files can be access and exploited by malicious agents, as most cloud service users assume no form of data protection.

Conclusions

We consider that companies should pay more attention to issues related to consumer privacy online, with ensuring appropriate information and obtaining consumer consent in collecting, processing and usage of personal data for business development.

Unfortunately we can make the conclusion that usage of cloud, cookies in relation with privacy in Romania is not taken in consideration by the consumer. People do not think very much about the privacy and they pass very easy on numerous occasions without taking any step to ensure their protection.

The attraction of the cloud is being on a platform that appears to offer unlimited computing resources. However, the same controls that are managing your enterprise infrastructure are also managing others at the same time, all on the same network. This high-wire act can create a scenario where even a minor glitch or breach could set off a string of consequences. The challenge then for cloud providers is whether they can keep on top of a complex and sizable network. The more users on that network, the more difficult it is to troubleshoot, the greater likelihood of a cloud blackout that impacts all the infrastructures tied throughout it. Even a successful incident response will likely involve shutting down large parts of the network, impacting you even if your infrastructure is not the source or primary victim of the problem.

Acknowledgement

The authors of this paper would like to thank the UEFISCDI (Executive Unit for Financing Higher Education, Research, Development, and Innovation) for the support provided in conducting this research and the dissemination of its results.

References

1. Allen, A.L., (2005). Privacy, in LaFollette, H., 2005, The Oxford Handbook of Practical Ethics, available at: books.google.ro/books?isbn=0199284237.
2. Gurau, C., (2008)., Integrated online marketing communication: implementation and management. *Journal of Communication Management, 12*(2), 169-184.
3. Ion, I., Sachdeva, N., Kumaraguru, P., & Capkun, S., (2011)., Home is safer than the cloud!: privacy concerns for consumer cloud storage. *Proceedings of the Seventh Symposium on Usable Privacy and Security, New York*, 797-802.
4. Pope, J.A., & Lowen, A.M., (2009). Marketing implications of privacy concerns in the US and Canada. *Direct Marketing: An International Journal, 3*(4), 301-326.
5. Veghes, C., Pantea C., Bălan D., & Rusescu, M., (2010). Attitudes of the consumers regarding the processing and employment of their personal data. *Annals of the University of Oradea – Economic Studies TOME XIX, 1*, 797-802.
6. Winer, R., (2009). New Communications Approaches in Marketing: Issues and Research Directions. *Journal of Interactive Marketing, 23*(2), 108-117.
7. *** - European Network and Information Security Agency (ENISA), 2011, Romania Country Report, available at: http://www.enisa.europa.eu/activities /stakeholder-relations/files/country-reports/Romania.pdf.
8. *** - Internet Society, 2012, Data Privacy On A Global Scale: Keeping Pace With An Evolving Environment - A roundtable organized by the Internet Society at the WSIS Forum 2012 – Geneva, available at:

http://www.internetsociety.org/sites/default/files/Data%20Privacy%20on%20a%20global%20scale_0.pdf