New rules on consumer protection against personal data breaches and spam

Panayiots Kitsos ,

Lawyer, PhD Candidate in the University of Macedonia - Department of Applied Informatics.

Key words: Privacy, Directive 2002/58/EC, Data breach notification, Cookies , Unsolicited Communications

1. Introduction

The rapid evolution of Information and Communication Technologies has significantly altered the way information is being stored and used. In particular as noted by Yves Poullet, the development of information technology is characterized by three elements; firstly, the constant growth of the capacity of computers, user terminals and the communication infrastructure (the so-called Moore's Law); secondly, the Internet revolution, and the subsequent convergence of the network around a single interoperable platform, the appearance of the 'Semantic Web' and Web 2.0 and the changes in identification and authentication techniques; thirdly the emergence of ambient intelligence that takes technology and the network and puts that technology and puts the technology into our everyday life, [Yves Poullet 2009].

Especially the use of the Internet and electronic filing systems have changed dramatically the way personal information is being viewed , by all sorts of entities such as universities, schools, hospitals, government agencies, corporate entities, and individuals , allowing virtually anyone to be able to access vast amounts of information regarding personal data. [Clifton 2009]. As noted "information....has passed from being an instrument through which acquire and manage other assets to being a primary asset it self"[Gindin 1997]. Corporations and marketers are collecting data which "extends beyond information about consumer's views of the product to information about consumers themselves, often including lifestyle details and even a full-scale psychological profile" [Solove 2004]. Social security numbers, credit-card numbers, medical records , e-mails and every information that can be defined as personal data can now easily be stored , processed, for illegal purposes or from unauthorized third parties. As a result data breaches and identity theft threaten the privacy of citizens and often resulting in considerable costs for business and other organizations.

The collection of these types of data is made possible with the help of the so-called "Cookies", which "have often been associated with potential security breaches, unauthorised transaction monitoring and privacy breaches" [Mitrakas 2006].

"Cookies" are small pieces of text files that are sent and placed by web servers to a user's computer, so that the users may be identified every time they log on to that web

server enabling web sites to be personalised by remembering the users preferences [King 2003] . The information that is collected does not necessarily identify a specific individual. “However, when combined with on-site registration data, which the Internet user provides when visiting some sites, cookie data may be used to build a profile of the specific Internet user”. [Gindin 1997]. The main arguments against cookies is that internet users are unaware of cookies and the fact that their personal data is being collected, without their prior knowledge or consent usually for direct marketing purposes [Munir 2005]

In addition to these internet technologies posing a threat privacy, the unwanted e-mail marketing the so-called “spam” which has bee defined as “(…)the bulk-mailing, sometimes repeatedly, of unsolicited e-mail messages, usually of a commercial nature, to individuals with whom the mailer has had no previous contact and whose email addresses the mailer collected from the public spaces of the Internet: newsgroups, mailing lists, directories, web sites etc” [CNIL 1999], at [Gauthronet, Drouard 2001], is a constant cause of unease for regulators and consumers.

Still data security breach and identity theft is regarded as one of the most important threats to privacy, which has a severe effect on the evolution of Information Society.

On May 28, 2010, the UK Information Commissioner’s Office issued a press release stating that it has been notified of more than 1,000 data security breaches since it began keeping records in late 2007(U.K's Information Commissioner Officer). This incident which was just one in a series of data breaches in UK raised the question first, of the need to view and manage data security at an organization wide level, and treat the problem as a priority by senior management. Secondly, that “while organizations generally understand that technology is a business enabler, they are still failing to recognize that it is also a risk” [Turle 2009].

Another recent data security breach event took place in Finland where data that were stolen from an Helsinki business in January 2010 exposed more than 100,000 payment cards. A small number of the compromised cards have been used to conduct fraudulent transactions.

These cases are just an example of the immensely growing problem of data security breach and identity theft the latter which is the fastest growing type of fraud in the United States. In 2008 about 9.9 million Americans were reportedly victims of identity theft, an increase of 22% from the number of cases in 2007. These incidents raise consumers concerns over the possibility of misuse of their personal data resulting thus to lowering confidence in internet transactions. Consumer confidence can then be gained only when electronic communication and internet service providers enhance security features of their services [Finklea 2010].

The problem is attempted to be addressed through a system of notification of those breaches. Notification has been seen as an important way towards the development of data security since it has been driving investment in data security within provider entities and allowing affected individuals to mitigate their damages [Dhont Woodcock 2010]. Also by alerting their bank, their credit card merchant, the National Regulatory Authority and law enforcement agencies; 'they can close unused financial accounts; they can place a credit freeze or fraud alert on their credit report”, not to mention that these notifications “can also enable law enforcement, researchers, and policy makers to better understand which firms and sectors are best (worst) at protecting consumer and employee data” [Romanosky, Telang, Acquisti 2008],

Moreover the right to be notified, as the right of the consumer to know when their personal information has been stolen or compromised [Maurushat], is enabling individuals to take steps to protect themselves from any harmful effects of the breach. Other justifications include the increase of "accountability" of organizations that suffer breaches, rising "awareness among the public," and "allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints"[Cate 2008].

In U.S.A exist various Data Breach Notification laws. The first State to have enacted data breach notification laws was California with the California Computer Security Breach Notification Act (S. B 1386), which came into effect on 2003. Since then most of the States have introduced similar laws . As a result U.S and international companies started to be more careful when using personal data, realizing that lack of security measures could seriously jeopardize their reputation and business.

In Europe even though data privacy has been heavily regulated offering European citizens an adequate legal framework to protect their personal data, still, prior to the new amended e-privacy directive , European consumers had no right to know "when their information has been tampered with or leaked illegitimately to a third party as the result of a security breach"(Cooper, Fink, Jones, Van Quathem 2006).

The growing numbers of data breaches led European Union in recognizing the importance of identifying and managing , data breaches through the existing legal framework .

On 25 November 2009, the European Parliament and Council adopted a new legislation to revise the regulatory framework for the electronic communications sector. This legislation includes Directive 2009/136/EC, which amends earlier Directive 2002/58/EC in the fields of 1. Mandatory notification of personal data security breaches, 2. Consent requirements for cookies and 3. Anti-spamming measures by ISPs.

The scope of the Directive is to enhance the protection of consumers privacy and personal data in the electronic communications sector, through strengthened security-related provisions and improved enforcement mechanisms by the NRAs .

2. Data security law in the European Union

Data Security in the European Union has been regulated by two Directives : Directive 95/46/EC,("Data Protection Directive"), and the newly amended Directive 2002/58/EC,4 on ("Privacy and Electronic Communications Directive").

2.1 Directive 95/36/EC

In Data Protection Directive, article 17(1) of the Data Protection Directive requires the "controller", processing personal data in the European Union to implement "appropriate technical and organizational measures" to protect any personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

In particular states that: “having regard to the state of art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected”.

According to Cooper, Fink, Jones and Van Quathem, the use of the word “appropriate” is in line with the scope of the Directive. “This was, however, intentional, since otherwise any specific security provisions rapidly would have become outdated. Instead, the Directive merely requires organizations to consider available technologies, their associated costs and the harm that would arise from unauthorized disclosure of or damage to personal data. In other words, organizations processing sensitive personal data will be expected to put in place more robust security measures” [Cooper, Fink, Jones , Van Quathem 2006].

Article 17(2) sets out additional conditions requiring the data controller “where processing is carried out on his behalf” to choose “a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures”

Article 17 (3) stipulates that the carrying of the processing has to be done by a written contract or other binding legal act in place between the data processor and any third party that processes personal data on its behalf.

2.2 Directive 2002/58/EC

Directive 2002/58/EC supplements the Directive 95/46EC aiming at protecting the fundamental right of privacy of natural persons in the field of electronic communication services ensuring the free movement of such data in the Community.

Article 4 of the Directive restates the provisions of Directive 95/46/EC requiring providers of a publicly available electronic communications service, to take appropriate technical and organizational measures to safeguard security of their services. In paragraph 2 we can observe that Directive stipulates the information the subscribers by the providers of a publicly available electronic communications service in case of a particular risk of a breach of the security of the network.

However it does not impose any “obligation to inform or notify the consumers of an actual breach, such as, for example, theft of credit card information”[Cooper , Fink, Jones , Van Quathem 2006].

The need for Europe to enhance internet security and tackle data breaches through security breach notification systems that had already been introduced in U.S.A started to be more than urgent and led to an intense debate that resulted to the new eprivacy directive provisions

3. The new ePrivacy Directive

As amended, by Directive 2009/136/EC the new E-Privacy Directive introduces an obligation to notify individuals and Authorities in instances of information security breaches.

3.1 Personal data breach

Directive 2009/136/EC provides with the concept of "personal data breach" which according to the Directive is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community." "[Directive 2009/136/EC];

"Personal data" has been defined as any data relating to an identified or identifiable individual, which is any data that may be linked to individuals through other information even where that information is held by another person [Directive 95/46/EC]

As it is stated in the second opinion of European Data Protection Supervisor this definition is welcome "insofar as it is broad enough to encompass most of the relevant situations in which notification of security breaches might be warranted". [EDPS 2009]. In addition, EDPS stresses the fact that this definition could "also include situations where there has been a loss or disclosure of personal data, while unauthorized access has yet to be demonstrated". As an example of possible personal data losses, according to EDPS are CD-ROMs, USB drives, or other portable devices or other situations where personal data have been made publicly available by regular users such as employee data file made inadvertently and temporarily available to a publicly accessible area through the Internet.

It is important though to make a reference to the definition of personal data according to the above mentioned "California Computer Security Breach Notification Act" which defines "personal information" as an individual's first name or initial and last name in combination with one or more "data elements," if either the name or the data elements are not encrypted. These data elements are: social security number (SSN); driver's license or state identification card number; or account, credit card or debit card number in combination with any required security code or password that would permit access to an individual's financial account. This rather restrictive approach is believed to produce better results when it comes to the notification procedure since it avoids over-notification.[Retzer 2008]. In any case this issue is about to be determined by the National legislations that will implement the Directive.

3.1.1 Field of Application

According to the new provision of the directive, article 3 of the Directive 2002/58/EC is replaced by the following provision

"This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.";

It is clearly stated that the provisions of the Directive apply to providers of "publicly available electronic communications services". The term is defined in Directive 2002/2/EC1 as "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not

include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

Thus the Directive applies to providers of public electronic communications networks and services,(PPECS) i.e. telecom operators, mobile phone communication service providers, internet access providers, providers of the transmission of digital TV content" [Dhont , WoodcocK 2010].

It must also be noticed that in the preamble of the Directive in Recital 55 is stated that the directive "does not apply to closed user groups and corporate networks." However is a point which lacks further clarification and it might be interpreted in many different ways .

As the article 29 Working Party notices in its 2/2008 opinion it is not always easy to distinguish public service from a private one.
Foe example hoe can we reach the correct definition when for example, internet access is provided by a multinational company, to 300.000 employees? Should it be treated differently if it is provided by a cybercafé?

Since this point has been debated a lot through the whole procedure it is important to note though, that the Article 29 Working Party and the European Data Protection Supervisor have proposed a broader application of the notification regime which should also include providers of information society services such as on-line banks, on-line businesses, on-line providers of health care services etc.

Especially in it's second opinion EDPS stresses that are two reasons why the application of the notification procedures should be extended to Information Society Service Providers (ISSP's). Firstly by setting the example, of United States where almost all of the States have enacted laws on security breach notification "which have a wider scope of application, encompassing not only PPECS but any entity holding the required personal data." Second by underlying that is not just personal data processed by PPECS that maybe breached, but all the types of personal and highly confidential information processed by ISSPs (i.e bank accounts, health-related information) could easily be disclosed, thus enabling the use for identity theft purposes[EDPS 2008].

Directive 2009/136/EC has a two fold approach on this issue. The European legislature is expressing a clear opinion on the preamble of the Directive supporting the expansion of notification requirements, as the "interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority." [Directive 2009/136/EC]. It is evident that even though this is not expressed in the wording of the main text still has a particular importance and might be seen as an encouragement of the Member States, towards the extension of the notification requirements to Information Society Service Providers (ISSP's), when implementing the provisions of the Directive.

3.1.2 Notification obligations

European legislature added three new paragraphs on article 4 of the Directive 2002/58/EC. The new provisions that are being added in article 4, provide that in the case of a personal data breach, a notification must be made to the competent authorities,

subscribers and other affected individuals.

In particular the Directive requires that the providers of publicly available electronic communications services, without undue delay, should notify the personal data breach to the competent national authority. This will have to be done irrespective of their possible harm [Van Quatherm 2010].

In addition when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider should also notify the subscriber or individual of the breach without undue delay. This is particularly important since if data breach is not addressed in an adequate and timely manner, could result in substantial economic loss and social harm, including identity fraud, to the subscriber or individual concerned [2009/136/EC].

It should also be noted though that according to the provision if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so [Directive 2009/136/EC]. This provision clearly provides that data breach should be notified not only to subscribers but also to other
Individuals affected by a certain data breach. This raises concerns over how this would work in practice since the service providers usually only have contact details of their subscribers . Of course as notes is rather possible that the intention of the Directive is to "cover users of ECSs that are not ''subscribers'' but with whom the service provider does have contact, and thus can easily be contacted in case of a breach"[Van Quathem 2010].

3.1.3 Content of the notification

The notification to the subscriber or individual should describe, i) the nature of the personal data breach, ii) the contact points where more information can be obtained, iii) should recommend measures to mitigate the possible adverse effects of the personal data breach and finally iv) when the providers notify the data breaches to the competent national authority should also, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach[Directive 2009/136/EC]

3.1.4 Exceptions

Nevertheless the notification to a subscriber or individual concerned is not required if the provider has demonstrated that it has implemented appropriate technological protection measures and the measures were applied to the data concerned by the security breach.
It is stressed that the technological protection measures should ensure that "personal data can be accessed only by authorised personnel for legally authorised purposes, and that the personal data stored or transmitted, as well as the network and services, are protected thus rendering the data unintelligible to any person who is not authorised to access it [Directive 2009/136/EC].

3.1.5 Competences of National Authorities

A new paragraph is also added regarding the competences of National Authorities. Under the new regime the competent national authorities can i) adopt guidelines ii) issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made and iii) they should also be able to audit whether providers have complied with their notification obligations under this paragraph, and

impose appropriate sanctions in the event of a failure to do so[Directive 2009/136/EC].

In addition providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of the Directive [Directive 2009/136/EC].

National Authorities won't be left alone to control the function of the new notification regime, since in order to ensure consistency in implementation of the provisions of the Directive, the Commission may, following consultation with the European Network and Information Security Agency (ENISA), the article 29 Working Party and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements[Directive 2009/136/EC].

3.2 Tracking technologies

Directive 2002/58/EC required Member States to implement restrictions on the use of hidden identifiers to "trace the activities of the user" on electronic communication networks acknowledging that devices such as cookies, "can be a legitimate and useful tool, for example, in analyzing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions" as long as users were provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices and had the opportunity to refuse to have a cookie or similar device stored on their terminal equipment.

These provisions of the e-Privacy Directive were largely welcomed; "it was seen to legalize the use of cookies while providing a degree of consumer protection against hidden tracking"[Brunger, Watts 2010]

The new provisions of the e-Privacy Directive require websites to seek consent before placing "cookies" and similar devices such as spyware (hidden espionage programs) and Trojan horses (programs hidden in messages or in other software), on a user's computer.

In particular article 5(3) of the Directive 2002/58/EC is replaced. The Directive adopts the "opt in" approach when addresses the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber. From now on access and storing of information is only allowed "on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing." In addition in the preamble of the Directive is provided that "user's consent to processing may be expressed by using the appropriate settings of a browser or other application."

The new provision provides exceptions to the "opt-in" regime, allowing the storage "where a cookie is necessary for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service "explicitly requested" by the subscriber or user to provide the service."

3.2.1 Implications for on-line advertising

A number of serious questions have been raised in relation to the "opt-in" requirements. Marketers and advertisers are particularly worrying on the effect that the new

provisions might have on their business. A number of questions have been raised in accordance to the implementation of these provisions. Firstly it has been raised the question relevant on the acceptance of the consent of the subscribers and users. Should each website have a certain page in which it provides information about its cookies? Should websites offer consent for each cookie, or each type of cookie used by the website? How should be interpreted recital 66 of the preamble of the Directive where it is clearly stated "The methods of providing information and offering the right to refuse should be as user-friendly as possible." Does this means that the "opt - out "regime still is in force and "if this is the case, then what is the difference with the current state, and what did the amendment intend to accomplish [itlawgroup]

In 2010 the Article 29 WP adopted Opinion 2/2010 on online behavioural advertising attempting to clarify the new provisions of the amended eprivacy Directive concerning the placing of cookies and other tracking devices.

The Opinion notes that advertising network providers should firstly obtain the informed consent before the placing of cookies or similar devices. Second consent must be obtained only after prior information about the sending and purposes of the cookie has been given to the user. Third consent "must be, freely given, specific and constitute an informed indication of the data subject's wishes". Fourth consent must be revocable [Article 29 WP 2010]. Furthermore in the Opinion the Article 29 WP requires from advertising network providers to create prior opt-in mechanisms such as "browsers or other applications which by default reject 3rd party cookies and which require the data subject to engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific web sites ….." and the conveyance of " clear, comprehensive and fully visible information in order to ensure that consent is fully informed". This can only be done if "the browsers convey, on behalf of the ad network provider, the relevant information about the purposes of the cookies and the further processing". The Article 29 WP considers that users' single acceptance to receive a cookie could also entail their acceptance for the subsequent readings of the cookie, and hence for the monitoring of their internet browsing. Thus, to meet the requirements of Article 5(3) it would not be necessary to request consent for each reading of the cookie [29 WP 29 2010].

As stated above on-line advertisers and Marketers are particularly worried with the new provisions concerning cookies and expect the implementation at National Level to see how the new e-Privacy Directive will finally be implemented. A fear exists that if Directive is implemented based on the wording of the main text, that will probably have negative consequences for free internet services such as Facebook, YouTube and Spotify that "rely on the revenue generated from online advertising space"[Brunger Watts 2010] as this will be forced to quit anonymous tracking of users habits.

In response to the 2/2010 Opinion it has been noted that an overly strict interpretation of the ePrivacy directive, would "kill any chance of the media building viable advertising revenues online and our serious efforts to give consumers effective control over the use of cookies" [Mills], the Internet in Europe would become less attractive to users something that would significantly undermine the growth potential of the digital economy and jeopardize the existence of European online companies finally calling into "question the EU's ambitious Digital Agenda, intended to increase Europeans access to ultra fast Internet and fostering the e-commerce sector" [WFA 2010]

Still as stated in the preamble of the Directive 2002/58/EC "Terminal equipment of users of electronic communications networks and any information stored on such

equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned" In addition the basic internet technology allows ad-network providers to easily track data subjects across different websites and over time gather and analyze their surfing behaviour in order to build extensive profiles about data subjects' interests.
The profiles that have been gathered are able to single out internet users and potentially harm their privacy.

3.3 Unsolicited Marketing Communications

In addition to the provisions regulating the use of cookies, the new ePrivacy Directive amends article 13 of the Directive 2002/58/EC extending the scope of the Directive. Member States should provide that unsolicited commercial messages may be sent to subscribers and users unless they have previously opted-in to receive the message.

In particular stipulates that "The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent."

The wording of Article 13.1 makes the assumption that the person is already connected to the network on which the communication is conveyed. It does not cover cases "where a solicitation would ask a user to connect to a network that serves advertisements exclusively. This may typically be the case in Bluetooth marketing applications" [WP 29 opinion 2009]

.

This observation has been taken into account in the preamble of the Directive is stated that "Safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail should also be applicable to SMS, MMS and other kinds of similar applications" ensuring that prior consent is required in Bluetooth marketing applications,

Still a natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that i) the contact details are obtained from the customers in the context of the sale of a product or a service, ii)the contact information must be obtained in accordance with Directive 95/46/EC, iii) the customers "clearly and distinctly are given the opportunity to object, free of charge and in an easy manner", iv) the customers are given the opportunity to object at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

At the end of the amended article 13(6) of the ePrivacy Directive states that any natural or legal persons that have been adversely affected by infringements of national provisions adopted pursuant to the new Directive provisions, have the right to bring legal proceedings in respect of such infringements in order for them to seek the cessation or prohibition of such infringements. This new provision it has been seen as an important step towards the protection of both natural legal persons (such as

consumer associations and trade unions representing the interest of spammed consumers)and PPECS against spammers since it allows Internet access providers to tackle spammers for abusing their networks, to sue entities counterfeiting sender addresses or hacking servers for use as spam relays[EDPS 2008], and thus defend the interests of their customers, as part of their own legitimate business interests.[Directive 2009/136/EC]

4. Conclusions

The introduction of the new amended provisions in Directive 2001/58/EC is definitely the right step towards the strengthening of the personal data protection. Data breach notifications, expansion of the “opt-in” system regarding the acceptance of cookies and similar devices, anti-spam provisions and the right to bring legal proceedings against spammers, they all form a “security-shield” necessary to protect consumer privacy and the development of on-line transactions.

Considering data breach problem is a rather complex and crosses all sectors there are more to be done and should not be addressed only in the frame work of electronic communications. As it is stated in paragraph 59 of Directive 2009/136/EC "Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC regardless of the sector, or the type, of data concerned."

The regulation of tracking technologies (spam and similar devices) raises important concerns amongst the advertisers since it affects their ability to receive feedback on consumers browsing history making difficult targeted and behavioural advertising.

In relation to unsolicited electronic marketing communications protection includes not only users but subscribers as well. Moreover is established the opt-in system in relation to unsolicited marketing communications sent via communications systems.

As stated above the amended Directive is definitely a step towards the right direction but it might not be enough.
As electronic communications become more and more complex, consumers become more aware about their privacy. Still their privacy concerns might lead to a diminished use of Internet transactions and subsequently to a loss of revenue for e-commerce.
Therefore companies and internet providers should invest on security technology since in an environment of technology the answer to privacy problems cannot be regulation alone.

REFERENCES

Brunger James, Watts Mark **“** Changes to the European E-Privacy Directive, Consequences for Online Advertising” http://www.bristows.com/?pid=46&nid=1494&level=2 (The attached article was first published in the Privacy & Security Law Report by The Bureau of National Affairs, Inc.) (accessed 12.5.2010)

Cate Fred (2008), “Information Security Breaches: Looking Back & Thinking Ahead” The Centre for Information Policy Leadership http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf.(accessed on 11.6.2010)

Clifton Phua (2009) “Protecting organisations from personal data breaches” Computer Fraud & Security , Pages 13-18

Commission Nationale de l’Informatique et des Libertés (2002) “Opération ‘Boîte à spams’: Les enseignements et les actions de la CNIL en matière de communications électroniques non sollicitées,” report submitted by Ms. Cécile Alvergnat and adopted 24 October 2002. http://www.cnil.fr/fileadmin/documents/approfondir/rapports/boite_a_spam.pdf(accessed on 1.6.2010)

Cooper Dan , Fink David. Jones Emile , Van Quathem Kristof (2006). “Security Breach Notification in Europe on The Orizon” World Data Protection Report , 10/06 http://www.cov.com/files/Publication/69e65c7e-4d08-474e-853b-3635e9120777/Presentation/PublicationAttachment/4064434a-7a6e-419e-89963c810d88da9c/757.pdf(accessed on 1.6.2010)

Dhont Jan, Woodcock Katherine (2010) “New Security Breach Notification Requirements Under Amended E-Privacy Directive” http://www.lorenz-law.com/wp-content/uploads/021-Notification-requirements-under-amended-E-Privacy-Directive-19012010.pdf. (accessed on 1.6.2010)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Official Journal L 201 , 31/07/2002 P. 0037 – 0047

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , Official Journal L 281 , 23/11/1995 P. 0031 – 0050

Finklea Kristin. (2010) “Identity theft : Trends and Issues” Congressional Research Service Report 1/2010, http://assets.opencrs.com/rpts/R40599_20100105.pdf(accessed on 1.6.2010)

Gauthronet Serge Drouard Etienne (2001) “Unsolicited Commercial Communications and Data Protection” (Internal Market DG – Contract n° ETD/99/B5-3000/E/96) January 2001, Commission of the European Communities http://www.rigacci.org/docs/biblio/online/spam_garante/document/434683.pdf (accessed on 1.6.2010

Gindin Susan(1997). “ Lost and Found in Cyberspace-Informational Privacy in the Age of the Internet”34 San Diego Law Review 1153

It Law Group (2010),“What's Cookin' in the European Union?” http://www.itlawgroup.com/index.php/resources/publications/169-of-cookies-and-spam?format=pdf (accesed 30.5.2010)

King Ian (2003) “On-line privacy in Europe—new regulation for cookies” , Information & Communications Technology Law, Volume 12, Issue 3 October 2003 , pages 225 - 236

Maurushat Alana (2009) "Data Breach Notification Law Across the World from California to Australia"(accessed on 11.6.2010)

Mitrakas Andreas (2006) “ Information security and law in Europe: Risks checked?” Information & Communications Technology Law, Volume 15, Issue 1 March 2006 , pages 33 – 53

Munir Abu Bakar
Protection; Never Mind the Rules Privacy and Data Protection: International and Regional Instruments 20th BILETA Conference: Over-Commoditised; Over-Centralised;Over-Observed: the New Digital Legal World?
Page 1 of 12 http://www.bileta.ac.uk/Document%20Library/1/Protection%20-%20Never%20Mind%20the%20Rules.pdf (accessed on 12.6.2010)

Opinion 2/2010 on online behavioral advertising , Article 29 WP ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/**2010**/wp171_en.pdf

Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) Article 29 WP http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf

Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive) http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf

Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications (2008/C 181/01) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consult

ation/Opinions/2008/08-04-10_e-privacy_EN.pdfPoullet Yves " Data protection legislation: What is at stake for our society

Poullet Yves " Data protection legislation: What is at stake for our society and democracy?" comp u t e r law & s e c u r i t y r e v i e w 2 5 (2 0 0 9) 2 1 1 – 2 2 6

Romanosky Sasha, Telang Rahul, Acquisti Alessandro (2008) "Do Data Breach Disclosure Laws Reduce Identity Theft? Seventh Workshop on the Economics of Information Security, June, 2008. http://weis2008.econinfosec.org/papers/Romanosky.pdf. (accessed on 1. 6.2010

Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2009/C 128/04) point 19

Solove Daniel (2004) "The digital person: technology and privacy in the information age", http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text/Digital-Person-CH2.pdf(accessed on 1.6.2010)

Turle Marcus (2009) "Data security: Past, present and future" Computer Law & Security Report, Volume 25, Issue 1, 2009, Pages 51-58

Van Quatherm Kristof (2010) . "Security breach notification in the European Union: First step taken, more to come" 01/10 World Data Protection Report BNA http://www.cov.com/files/Publication/3c4eadcd-c074-44f8-925f-4a63d5304d70/Presentation/PublicationAttachment/9c8fb8a0-b55a-4464-ac4b-4a7722eda833/Security%20breach%20Notigication%20in%20the%20EU%2c%20first%20step%20taken%2c%20more%20to%20come.pdf (accessed 11.6.2010)

World Federation of Advertisers (2010) http://www.wfanet.org/press_releases.cfm (accessed on 1.6.2010)