Spam, spamdexing and regulation of internet advertising

Paul Przemysław Polanski

Jean Monnet ad personam Department of European law,
Faculty of Law, Warsaw University, Poland
E-mail: ppolanski@wpia.uw.edu.pl

Abstract: The European Union has developed a rather comprehensive regulatory framework concerning advertising on the internet. However, these developments have had an impact primarily on the European Economic Area and the candidate countries, such as Turkey. On a global level, there is no international regulation dealing with questions as to how to advertise in cyberspace. As a result, these matters are primarily governed by international trade usages or cyberspace customs. The aim of this paper is to present certain practices that have emerged in internet industry, which supplement the Community regulatory framework.

Keywords: spam; spamdexing; internet advertising; commercial communication.

Reference to this paper should be made as follows: Polanski, P.P. (2008) 'Spam, spamdexing and regulation of internet advertising', *Int. J. Intellectual Property Management*, Vol. 2, No. 2, pp.139–152.

Biographical notes: Paul Przemysław Polanski (PhD, BBus, Magister Prawa) is a Lawyer and a Software Engineer. Presently a Senior Researcher in the Jean Monnet *ad personam* Department of European Law, Faculty of Law, University of Warsaw and in the Department of Information Systems, Leon Koźmiński Academy of Entrepreneurship and Management (LKAEM), Warsaw. Previously, he worked as a Computer Programmer in Australian IT industry and as a researcher at the University of Melbourne and Monash University. Currently, he manages a development of legal information system at C.H. Beck and administers e-learning platforms.

1 Introduction

Electronic commerce continues to evolve without a detailed set of laws on a global and regional level. It is visible in the area of internet advertising, which remains completely unregulated. So far, international community has only managed to adopt a general framework concerning copyrights in the Information Society (WIPO, 1996a, 1996b) and the Convention on Cybercrime (Council of Europe, 2001). All of these instruments have had a very limited impact on the functioning of the internet and online advertising. In 2005 United Nations adopted a Convention on the Use of Electronic Communications in International Contracts (United Nations, 2005), but it has not entered into force yet. Besides, it is not concerned with internet advertising at all (Polanski, 2006b).

On the other hand, internet merchants continued to trade and develop new marketing techniques. The lack of clearly defined legal framework could not stop them from entering the new marketplace. Despite the initial strong resistance of internet community to commercial advertising, electronic marketing of goods and services soon became a commonplace. One of the earliest technologies employed to advertise online was electronic mail. Soon, mass marketing followed. Some of the marketers decided to conceal their true e-mail addresses, therefore engaging in what is now known as a malicious spam. Such unsolicited commercial communication became a true plague on a global scale. Soon spamming affected other internet applications, particularly discussion forums, guestbook and recently, blogs and wikis. The lack of a legal framework forced companies, internet Service Providers and internet users to fight spam using filters and blocking their content – without a success, though. The new wave of graphical spam followed, which lasts till today.

At the same time, web companies decided to fight for a high listing on popular engines by resorting to other dubious practices. For instance, metatags became overloaded with references to competitors' trademarks and websites, in order to be listed higher. Hidden texts describing competitors' products or services were used as a technique to boost search results. Numerous 'junky' websites were created in order to create millions of links pointing to a target website with a hope of increasing the position of such a site. None of these techniques are forbidden or permitted by international law, although there is some case law in this area. However, search engines decided to self-regulate and to block websites that engage in such practices.

The aim of this paper is to discuss spam and spamdexing practices that have emerged in internet industry. Furthermore, issues that arise in the context of interactive advertising will also be highlighted. However, it is not intended to cover the whole spectrum of all legal issues that arise in the context of online advertising. For instance, problems associated with a right of an online company to accept or reject an advertisement will not be covered. Similarly, problems that arise with respect to context-based advertising, click frauds or linking to copyrighted or controversial materials will not be discussed. Furthermore, the conflicting judicial decisions with respect to whether a name used in a metatag violates trademark laws will not be analysed. The present contribution will focus on spamming, spamdexing and interactive advertising practices associated with promoting goods and services via websites and e-mail. The first part will briefly outline European Community legal framework concerning advertising. Then, potential trade usages or customs will be analysed, followed by a conclusion.

2 EU regulation of internet advertising

The European Union has developed a comprehensive framework concerning misleading and comparative advertising (OJ L 149/22, 11.06.2005; OJ L 250/17, 19.09.1984) and unfair commercial practices (OJ L 149/22, 11.06.2005). In addition, there are sector-specific regulations concerning commercial communication with respect to, for example, tobacco products (OJ L 152/16, 20.06.2003) or pharmaceuticals (OJ L 311/67, 28.11.2001). As far as e-commerce is concerned, tobacco products cannot be advertised online unless such communication is intended exclusively for professionals in the tobacco trade or an online communication has been published in third countries and

targeted there (Article 3). However, there are only few rules specifically devoted to electronic commerce.

Among those specific rules of internet-based commercial communication, one should mention the Directive 2000/31/EC on electronic commerce (OJ L178/1, 12.11.2000). It supplements the aforementioned regulations. The directive treats advertising as an information society service (OJ L204/37, 21.07.1998), which must be provided at a distance, by means of electronic equipment (practically limited to the internet) and at the individual request of a user. Activities of search engines or online portals are examples of information society services. To describe internet advertising the directive uses the term 'commercial communication', which is defined as

> "any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession."

The drafters were aware that commercial communications are essential for the financing of information society services and for developing new ones. Hence, it does not seem erroneous to equate commercial communication and advertising.

However, this instrument does not go beyond few general requirements such as- that a commercial communication and an advertising company be clearly identifiable. Therefore, online entrepreneurs are required to identify themselves and to clearly inform about the fact that a given communication is, in fact, advertising. Promotional offers (discounts, gifts, premiums) and promotional competitions or games shall contain conditions, which should be easily accessible and presented in a clear and unambiguous manner (Article 6).

On the other hand, Article 8 introduced a very important rule permitting the regulated professions to advertise online. In numerous European countries advertising by, for instance, a lawyer was prohibited. The newly adopted directive on services (OJ L 149/22, 11.06.2005) abolished this restriction and extended the protection offered by the directive on e-commerce to all media (Article 24). As a result, Member States shall remove all total prohibitions on commercial communications by the regulated professions and ensure that such communications comply with professional rules, in conformity with Community law, which relate, in particular, to the independence, dignity and integrity of the profession, as well as to professional secrecy, in a manner consistent with the specific nature of each profession.

As far as e-mail advertising is concerned, the Directive on electronic commerce introduced a rather unfortunate provision permitting the so called unsolicited communication or spam. The obligation put on spammers to identify their e-mails and to consult *opt-out* registers simply did not work. It took European institutions two years to realise that opt-out registries serve mainly as a source of confirmed e-mail addresses for spammers and therefore, the Directive 2002/58/EC introduced the so called *opt-in* model (OJ L201/37, 31.07.2002).

According to the new model, the prior consent of a natural person is required:

> "The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent." (Article 13(1))

The technologies covered embrace not only electronic mails or faxes but also SMS messages (recital 40). However,

> "other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls."

As a result, certain technologies, such as, internet telephony can be used for the purposes of direct marketing, although member states may uphold existing rules requiring the prior consent irrespective of the technology used.

The new system, however, contains some important exceptions. For instance, it is legal to send unsolicited e-mails, provided that a sender received a recipient's e-mail address in the context of the sale of a product or a service (Article 13(2)). Furthermore, the old *opt-out* system might apply in B2B transactions, because Article 13 of the directive applies to subscribers who are natural persons (Article 13(5)). As it was stated above, certain technologies can still be used without a user's prior consent. On the other hand, e-mail messages that conceal the identity of the sender or do not use a valid e-mail address are prohibited (Article 13(4)). Therefore, the malicious spam is prohibited irrespective of a legal status of a sender or a recipient. Unfortunately, introduction of the new model did not stop it.

In summary, the EU regulatory framework concerning advertising on the internet has had an impact primarily on the European Economic Area and the candidate countries, such as Turkey. On a global level, there is no international regulation dealing with questions on how to advertise in cyberspace. As a result, these matters are primarily governed by international trade usages or cyberspace customs.

3 Trade usages in online advertising

Unwritten customs or usages play a significant role in regulating transnational trade and international relations. For instance, the 1980 Vienna Convention on Contracts for the International Sale of Goods explicitly recognises their binding nature in Article 9(2), which states:

> "The parties are considered, unless otherwise agreed, to have impliedly made applicable to their contract or its formation a usage of which the parties knew or ought to have known and which in international trade is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade concerned."

As a result, trade usages that are widely known and regularly observed are binding irrespective of the knowledge of a given merchant. Trade usages are sometimes referred to as *lex mercatoria* (Mustill, 1987).

As far as inter-state relations are concerned, international custom is equally important source of law as a treaty. Article 38 of the Statute of the International Court of Justice defines international custom as "*evidence of practice accepted as law*" (UN, 1945). There are, therefore, two elements that must be ascertained: practice and its acceptance as law (*opinio iuris*). ICJ recognised numerous international customs, for example, in the area of treaty law, diplomatic relations, environment protection or the law of the sea (Wolfke, 1993).

Similarly, there are numerous customs or trade usages that have emerged on the internet, particularly with respect to online advertising. This area is particularly interesting because revenue that is generated by online marketing is the cornerstone of the majority of business models encountered on the net (Polanski, 2007, p.337). For instance, information portals or search engines rely mostly on advertising revenues to support their operations. These revenues come from, for example, online banners, sponsored links and to lesser extent from pop-up screens.

Internet trade usage can be defined as

> "a legally relevant practice of trading on the internet, which is sufficiently widespread within a given timeframe as to justify the expectation that it should be observed." (Polanski, 2007, p.9)

As in the case of international customs, it can develop quite rapidly. Usually it takes few years for a usage to be established but in certain case scenarios they can develop much faster (Polanski, 2006a). The practice is widespread if it has a global, regional or even a local character (widespread in space) and if it is followed intensively in time (widespread in time). In internet advertising, the practice has a global character if it is observed by the majority of online advertisers or publishers (arguably 75% or more). It can also exhibit a particular character if it is peculiar to a number of companies exhibiting some commonality, for example, companies that are confined to one or several industries (e.g., search engines) or to one or several geographical regions.

Courts and arbitrators should recognise widely known practices as trade usages and apply them to clarify contractual provisions or to fill in gap resulting from an absence of binding regulations or contractual provisions (Goode, 1997). In Western legal tradition, trade usages usually have interpretative and supplementary functions. In certain countries, however, custom is an independent source of law. For instance, in Switzerland, a judge should apply customary law in the absence of relevant statutory law (Gutteridge, 1971). Similarly, in Spain, custom operates in the absence of written law provided that it is proven and not contrary to morality or public order. On the other hand, English customs have to be immemorial (dating back to 1189), continued, peaceable, not unreasonable, certain, compulsory and consistent and proven as a fact (Blackstone 1783 reprinted 1978). American trade usages, in turn, must be regularly observed but do not have to be immemorial, reasonable or local (de Ly, 1992, p.138).

Taking into account the potential role of unwritten customs, it is particularly important to observe certain practices that have emerged in the area of internet-based advertising. These usages could fill in gaps resulting from a lack of international framework concerning advertising on the Net. The section below will present potential customs that have emerged in this field.

3.1 E-mail spam

In the early days of the internet, sending commercial e-mails was unthinkable.[1] When in 1994 a Phoenix law firm Canter and Siegel posted an immigration law advertisement on bulletin boards, the community of users reacted furiously and effectively blocked their e-mail account by sending thousands of e-mail messages. The law firm's account was soon revoked on the grounds that the company abused its privileges. As the system administrator of a company providing internet access to Canter & Siegel explained:"*They took 15 or 20 years of internet tradition and said the hell with it*" (Bodansky, 2004).

The early customary norm prohibiting commercial use of the internet proved transitory. Commercial advertising was finally accepted by the internet community.

> "Although violators suffered sanctions, these sanctions ultimately proved insufficient to serve as an effective deterrent. Instead, over time, the non-compliant behaviour established a new custom permitting advertising on the internet, and by now this behaviour no longer entails any penalties." (Bodansky, 2004)

This does not mean that all forms of commercial advertising have been accepted.

Certain advertising practices are still not tolerated. It is particularly so with respect to spam or unsolicited, bulky e-mail advertising that is difficult to block (Edwards, 2000, p.309). In general, the rules of Netiquette justify this prohibition in the following words:

> "The cost of delivering an e-mail message is, on the average, paid about equally by the sender and the recipient (or their organisations). This is unlike other media such as physical mail, telephone, TV, or radio. Sending someone mail may also cost them in other specific ways like network bandwidth, disk space or CPU usage. This is a fundamental economic reason why unsolicited e-mail advertising is unwelcome (and is forbidden in many contexts)." (Hambridge and Lunde, 1999; Hambridge, 1995).

The status of the Netiquette as a basis for adjudication of disputes has been confirmed in *Christophe G. v. Société France Télécom Interactive, S.A.*,[2] where a French court recognised the prohibition of spamming as a binding custom (Polanski, 2007, pp.138, 139).

One of the most evident examples of unwelcome (and forbidden) spam is bulky e-mail advertising that contains arbitrary sender addresses. It is difficult to fight this kind of spam, because a sender address keeps changing every time in order to avoid simple text filtering. Such examples of spam have never been tolerated by internet users and this attitude is common worldwide. It has also been recognised in Article 13 of the European directive on privacy and electronic communications, which outlaws this kind of spam in the following manner:

> "4. In any event, the practice of sending electronic mail for purposes of direct marketing, disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited." (OJ L201/37, 31.07.2002)

Similarly, Section 5 of the American 2003 CAN-SPAM Act prohibits false or misleading transmission information:

> "It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading." (15 USC 7704)

This Act also prohibits deceptive subject headings, e-mails that do not contain a functioning return electronic mail address and commercial advertising after objections.

However, there are spam messages that are even more difficult to fight, for instance, e-mails that contain advertisements in graphical format. Marshal estimates that in April 2007, 42% of spam was image spam.[3] The reason for embedding advertisement in a graphical image is to circumvent the operation of e-mail filters that can only operate on text. As a result, it is virtually impossible to stop companies that utilise this technique to

advertise their products. Unless advanced techniques are applied in the area of information filtering, internet users will have to bear graphical spam. One such technique, known as the Optical Character Recognition (OCR), has been used by scanning software to translate pictures of characters into computer fonts. However, even this technology has its limitations if the background and font colours of an advertisement are similar.

Another type of e-mail advertising that is particularly unwelcome and very hard to fight is spamming in order to undermine the network security. For instance, bulky e-mail messages are often used to spread viruses, Trojan horses or other dangerous software. Fortunately, nearly all e-mail server administrators use anti-virus software that deletes dangerous attachments before they reach client computers. One can therefore argue that it is a customary obligation of e-mail service providers to use anti-virus software on their servers in order to reduce the amount of spam and to fight the spread of viruses and other forms of malicious software. However, it is not the end of serious security issues posed by spam. Bulk electronic messages are also often used in order to forge Distributed Denial of Service (DDoS) attacks (Hambridge and Lunde, 1999, p.3), which result in temporary unavailability of internet services such as a website or an e-mail server. Hackers spam target servers in order to hack into computer systems. This use of spam is probably the most dangerous but is much harder to stop.

It is difficult to provide reliable estimate of e-mail spam as available statistics lack clearly defined methodology. Some authors argued that in 2006 40% of e-mail s were spam (Evett, 2007). As far as the type of spam is concerned, nearly 45% of spam messages were related to health. Other spam messages advertise certain financial deals, products, adult content, phishing, education and scams.[3] A lot of spam messages, though, contains randomly assembled content and is therefore completely useless.

For years almost all the spam originated in the USA (Edwards, 2000, p.310). However, recent statistics show that spammers look for other countries to continue their activities. According to the Spamhaus Project, as of April 2007, the USA remains the worst spam origin country, but China, Russia and UK are becoming increasingly more popular. Other spam havens include Japan, South Korea, Germany, Netherlands, Canada and Taiwan.[4] On the other hand, Marshall suggests that most spam originates from Europe "thanks largely to increasingly strong showings from Italy and Poland".[3]

The Spamhaus Project researchers also demonstrated that nearly 80% of spam targeted at North American and European population is generated by a group of around 200 known professional spam gangs, listed in Spamhaus' Register Of Known Spam Operations (ROKSO) database. On a weekly list of the top ten worst spammers and spam gangs dominate individuals or organisations from Russia and Ukraine, followed by Israel, Australia, Hong-Kong and USA.[5]

Spam has not been accepted by international community. The negative attitude or *opinio iuris* towards spam is visible in the works of international organisations that try to fight it. As an example, the Declaration of Principles adopted at the World Summit on the Information Society underlies the importance of fighting spam.

> "Spam is a significant and growing problem for users, networks and the internet as a whole. Spam and cyber-security should be dealt with at appropriate national and international levels." (WSIS, 2003, No. 37)

The Internet Research Task Force (IRTF) has established the Anti-Spam Research Group in order to investigate tools and techniques to mitigate the sending and effects of spam. In particular, the research group focuses on anti-spam tools and techniques that

> "include those to prevent spam from being sent, to prevent spam from being received, to distinguish spam from legitimate mail, to facilitate management responses to spam activity, and to ensure that legitimate mail is delivered in the presence of other anti-spam measures."[6]

Furthermore, the continuous development of technologies targeted at fighting spam is another proof of the common intention to get rid of it. The vast majority of internet users and probably all e-mail server administrators use spam filters in order to block the flood of unwanted electronic communications. This argument can serve as another proof of the customary nature of prohibition in respect to commercial spam.

In summary, there are plenty of legal, technical and organisational efforts to remove spam. These undertakings clearly signify the intention of the majority of users to block spam advertising that is generated by a very small fraction of the internet community. One can therefore argue that it is customary for online business to refrain from sending spam. It is a global customary obligation.

3.2 Spamdexing

Successful advertising on the WWW involves an appropriate modification of a webpage so that search engines would list it highly. A typical web user would not read beyond the first 10–20 search results. In consequence, a high ranking within the results of a search engine is critical for the success of an online business.

Spamdexing (or web spam) refers to spamming the index of a search engine. In other words, web spam refers to "*actions intended to mislead search engines into ranking some pages higher than they deserve*" (Gyongyi and Garcia-Molina, 2005, p.1). Although the term spamdexing is similar to spam, these two practices should not be confused. According to Wikipedia

> "spamdexing refers exclusively to practices that are dishonest and mislead search and indexing programs to give a page a ranking it does not deserve."[7]

Unfortunately, because of the financial gain in achieving a high search engine rank, the amount of spamdexing has increased dramatically, leading to a degradation of search results (Gyongyi and Garcia-Molina, 2005).

In the early days of WWW, search engines relied on matching queried keywords in available electronic documents. Such simple text searches were especially vulnerable to manipulation by repetition of targeted keywords on a page. Consequently, search engines abandoned this philosophy and the next generation of search engines used more sophisticated techniques. Lycos was first to develop the concept of 'implicit voting', which treated a link to a page as a 'vote' for it (Jones, 2005). As a result, a webpage with many links pointing to it would be more 'important' than pages with few links.

Google's PageRank algorithm has improved this concept with the notion of the 'importance' of a page. In consequence, pages that are referenced from often cited pages such as Yahoo would be given higher ranking than pages that might have more links but from more obscure places (Page et al., 1998, p.3). Therefore, "*for a page to get a high PageRank, it must convince an important page, or a lot of non-important pages to link to it*." (Page et al., 1998, p.12). However, despite its apparent immunity to manipulation, this concept has not turned out to be entirely bullet-proof. Google bombing,[8] which involves creating pages that directly affect the rank of other sites is used particularly in non-commercial settings, e.g., to ridicule political leaders (BBC News, 2003).

Furthermore, web spammers often create links from blogs, wikis or guestbook in order to increase the position of their sites.[9]

Spamdexing can take multiple forms. Common spamdexing techniques are classified into two broad classes: content spam and link spam (Gyongyi and Garcia-Molina, 2005, pp.3, 4).[10] With respect to content spam, keywords can be placed in various so called 'text fields': a body of a page, its title, meta tags, URL or anchor text. Depending upon the aim of a web spammer, a specific term can be repeated numerous times in these text fields or a great variety of words can be placed there. The content spam category includes techniques that place keywords as a hidden text (e.g., font colour is the same or similar to background colour). If such keywords are repeated in the body of a webpage one speaks of keyword stuffing. On the other hand, repeating keywords in meta tags is referred to as a meta tag stuffing. Other techniques include doorway pages, which contain very little content but are 'stuffed' with keywords and redirecting sites that redirect a user to a different website, without showing him the spammed website.

Link spam embraces even more techniques. A web spammer will be primarily interested in using his own pages and other accessible pages to link to. It is fairly easy to use a spammer's own sites to link to a target website to boost its ranking. However, web spammers will also try to link from pages maintained by others e.g., to link from a popular blog to a target website. As a result, spamdexing is closely associated with blog spam. The most common linking technique is link farm (or spam farm), which involves any group of web pages that all hyperlink to every other page in the group.[11] By creating large spam farms with all the pages pointing to the target, a spammer can boost Google's PageRank (Gyongyi and Garcia-Molina, 2005, p.5). Web spammers may also use invisible links in order to increase the importance of a page. Sometimes spamdexers purchase expired domains in order to replace the pages with links to their pages. There are also other techniques such as cloaking, which refers to presenting a different page to a web crawler than will be seen by human users (Jones, 2005). As with other practices, cloaking can be used for legitimate and illegitimate purposes.

Gyöngyi and Garcia-Molina (2005, p.8) estimate that 10–15% of the content on the web is spam. Spamdexing decreases the quality of search results and inflates search engines with useless pages therefore increasing the cost of processing queries (Gyöngyi and Garcia-Molina, 2005, p.1). Furthermore, it forces some honest webmasters to spamdex in order to be found. However, there is still a lack of technical measures for combating this. For instance, "Search engine SPAM detector" tries only the three most common spamdexing methods: keyword stuffing, doorway farms and hidden text.[12]

One of the major problems associated with spamdexing is that these techniques can be used for both legitimate and illegitimate purposes. There are numerous techniques that have been accepted in the industry as procedures for making a website indexable by search engines, without misleading the indexing process (known as search engine optimisation or SEO). SEO is a legitimate practice, however, most companies providing search engine optimisation services engage in spamdexing (Gyöngyi and Garcia-Molina, 2005, p.2). On the other hand, the most dangerous forms of spamdexing involve repeated use of certain keywords such as registered trademarks, brand names or famous names in one's webpage to take advantage of their goodwill. Such practices have been tested in courts worldwide and a consensus has emerged that they violate either competition laws (in Europe) or trademark laws (in USA) (Nathenson, 1998, Part II). In other cases, however, there is no law that explicitly deals with spamdexing.

In consequence, search engines have established and enforced their own web spam policies. Webmasters are usually provided with detailed guidelines that explain how to structure a webpage. For instance, Google specifies quality guidelines and warns that if a site does not meet them, it may be blocked from the index.[13] Similarly, Yahoo has designed Content Quality Guidelines "*to ensure that poor-quality pages do not degrade the user experience in any way*".[14] The company has reserved "*the right, at its sole discretion, to take any and all action it deems appropriate to insure the quality of its index*."

Based on the evidence of positive actions taken by internet users to fight spamdexing, one can argue that a new customary right has emerged permitting search engines to block web spam. It is too early, however, to speak about a customary obligation to refrain from spamdexing, because techniques such as cloaking or hidden text can be used for both legitimate and illegitimate purposes. However, this area is evolving rapidly and such customary obligation might emerge soon. Clearly, more research is required, particularly with respect to unfair competition laws and trademark laws, which seem most suitable to tackle some of the highlighted problems.

3.3 Web-based interactive advertising

With the advent of web-based advertising, new marketing practices have emerged. From the very beginning cookies were used to gather information about a user in order to deliver a personalised commercial content. Cookies are invisible files containing user's profile, which are sent by a web server and stored on the user's hard disk. A website then 'knows', for example, what username and password does a user have, what products were put in a shopping cart or which colours did a user select as a 'skin'. As directive 2002/58/EC stated in recital 25

> "… 'cookies' can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions."

Cookies are very important tools facilitating online interactivity, which raise serious privacy concerns. Technically, they are created, stored and transmitted to a web server without user's knowledge or consent and might contain sensitive data.[15] The aforementioned directive on privacy and electronic communications states that where cookies

> "… are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using."

As a result, an online entrepreneur should inform a user about the purposes of the cookies. Furthermore, website operator should give users the opportunity to refuse to have a cookie. Taking into account that modern browsers enable effective management of cookies, including deletion, one can argue that a customary norm has developed, which gives information society service providers a right to explore user's behaviour using cookies (Polanski, 2007, p.323).

On the other hand, in the early days of web marketing pop-up windows were often used that contained simplified animations and graphics. However, introduction of pop-up blockers diminished the significance of this form of online marketing. As a result, the market self-regulated this form of marketing and no intervention of legislator was necessary. However, with the widespread adoption of Macromedia Flash software that is being used to create animated introductions, ad banners and transparent animations similar problems have appeared. The latter form of multimedia advertising is particularly intrusive when the animation is very loud, occupies the whole screen and it is hard to find a way to get rid of it. However, the majority of such advertisements usually contain a 'close' button or similar means that allows the user to close the animation. It is therefore possible that a customary norm requiring online entrepreneurs to allow for closure of interactive advertising has emerged. However, at this stage it is too early to speak about a general custom requiring such behaviour. In addition, it is very difficult to say what remedies internet users would have, if a given online business decided not to provide such functionality.

There are numerous other practices and issues that should be covered under the heading of web-based interactive advertising. For instance, one should investigate the legality of sponsored links, which do not differ from 'normal' hyperlinks in a technical sense. Sponsored links have emerged relatively recently and proved to be very effective both for the advertiser and the site owner. Although they are widely used, their usage might conflict with trademark laws or unfair competition laws. However, the space does not permit to investigate all of these issues in depth.

4 Conclusion

There is no international law on advertising on the internet. Despite a well-developed regulatory framework in the European Union countries, certain internet practices are not covered by the legislation. The most important example is a practice of spamdexing or web spam, which is an extension of the 'traditional' spam found in e-mail messages. With respect to the latter, it is argued that online businesses are legally bound to refrain from spending spam based on a widely known and accepted internet custom. This statement is reinforced by legislation on a regional or country level. As far as spamdexing is concerned, it is argued that search engines have a right to block websites that contain web spam based on a widely followed trade usage. This right clearly supplements existing rights and obligations under the applicable law.

Furthermore, information society service providers have the right to explore the user's behaviour using cookies. This marketing practice has been accepted by the internet community, despite some privacy concerns. It is a very important trade usage concerning online marketing because modern WWW is dependant upon customisation and interactivity. Finally, it is customary for online entrepreneurs to provide means of closing interactive advertising such as pop-up screens or Flash animations. All of these trade usages supplement existing legal framework on a national, regional and international level but need to be tested in courts.

References

BBC News (2003) *'Miserable Failure' Links to Bush*, 7 December, Available at: http://news.bbc.co.uk/2/hi/americas/3298443.stm, Accessed: 08/04/2007.

Blackstone, W. (1783 reprinted 1978) *Commentaries on the Laws of England*, Garland Publishing, Inc., New York, London.

Bodansky, D.M. (2004) *Customary International Law: Diplomatic Immunities (electronic classes)*, Fall, Available at: http://www.law.uga.edu/~bodansky/courses/International_Law/class 12.html, Accessed: 28/08/2006.

Council of Europe (2001) *Convention on Cybercrime*, ETS No.: 185, signed at Budapest, 23 November, Available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, Accessed: 7/08/2006.

de Ly, F. (1992) *International Business Law and Lex Mercatoria*, TMC Asser Instituut – The Hague, , Amsterdam, London, New York, Tokyo.

Edwards, L. (2000) 'Canning the spam: Is there a case for legal control of junk electronic mail?', in Edwards, L. and Waelde, C. (Eds.): *Law and The Internet. A Framework for Electronic Commerce*, Hart Publishing, Oxford, pp.309–329.

Evett, D. (2007) *Spam Statistics 2006*, Available at: http://spam-filter-review.toptenreviews. com/spam-statistics.html, Accessed: 28/3/2007.

Goode, R. (1997) 'Usage and its reception in transnational commercial law', *International and Comparative Law Quarterly*, Vol. 46, pp.1–36.

Gutteridge, H.C. (1971) 'Comparative law', *An Introduction to the Comparative Method of Legal Study and Research*, Cambrdige University Press, Cambridge.

Gyöngyi, Z. and Garcia-Molina, H. (2005) *Web Spam Taxonomy*, Available at: http://airweb.cse. lehigh.edu/2005/gyongyi.pdf, Accessed: 28/08/2006.

Hambridge, S. (1995) *RFC 1855 Netiquette Guidelines (Also FYI0028)*, October, (Status: INFORMATIONAL), Available at: http://www.ietf.org/rfc/rfc1855.txt?number=1855, Accessed: 1/04/2006.

Hambridge, S. and Lunde, A. (1999) *RFC 2635 Don't Spew. A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*, June, (Status: INFORMATIONAL), Available at: http://www.ietf.org/rfc/rfc2635.txt, Accessed: 26/08/2006.

Jones, T. (2005) 'Both sides of the digital battle for a high rank from a search engine', *Association for Computing Machinery New Zealand Bulletin*, Vol. 1, No. 2, pp.1–6.

Mustill, M. (1987) *The New Lex Mercatoria: the First Twenty-five Years, in Liber amicorum for Lord Wilberforce*, M. Bos, Brownlie, I, Clarendon Press, Oxford, pp.149–182.

Nathenson, I.S. (1998) 'Internet infoglut and invisible ink: spamdexing search engines with meta tags', *Harvard Journal of Law and Technology*, Vol. 12, No. 1, Fall, pp.43–147.

OJ L 149/22 (11.06.2005) *Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market and Amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive')* (Text with EEA relevance).

OJ L 152/16 (20.06.2003) *Directive 2003/33/EC of the European Parliament and of the Council of 26 May 2003 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Relating to the Advertising and Sponsorship of Tobacco Products*.

OJ L 250/17 (19.09.1984) *Directive 84/450/EEC of 10 September 1984 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Misleading Advertising*.

OJ L 311/67 (28.11.2001) *Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community Code Relating to Medicinal Products for Human Use*.

OJ L178/1 (12.11.2000) *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce)*.

OJ L201/37 (31.07.2002) *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)*.

OJ L204/37 (21.07.1998) *Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations*.

Page, L., Brin, S. *et al*. (1998) *The PageRank Citation Ranking:Bringing Order to the Web*, 29 January, Available at: http://dbpubs.stanford.edu:8090/pub/showDoc.Fulltext?lang=en&doc=1999-66&format=pdf&compression=&name=1999-66.pdf, Accessed: 28/08/2006, pp.1–17.

Polanski, P.P. (2006a) 'Evidencing trade usages: the case of encryption practices in internet banking', in Kierkegaard, S.M. (Ed.): *Business Law and Technology: Present and Emerging Trends*, IAITL, Vol. 1, pp.365–386, Denmark, ISBN 87-991385-0-6

Polanski, P.P. (2006b) 'International electronic contracting in the newest UN convention', in Kierkegaard, S.M. (Ed.): *Business Law and Technology: Present and Emerging Trends*, IAITL, Vol. 1, pp.351–364, Denmark, ISBN 87-991385-0-6.

Polanski, P.P. (2007) *Customary Law of the Internet: In the Search of the Supranational Cyberspace Law*, TMC Asser Press, The Hague.

UN (1945) *Statute of the International Court of Justice*, 26 June, Available at: http://www.icj-cij.org/icjwww/ibasicdocuments/ibasictext/ibasicstatute.htm, Accessed: 23/03/2007.

United Nations (2005) *United Nations Convention on the Use of Electronic Communications in International Contracts*, 23 November, Available at: http://www.uncitral.org/pdf/english/texts/electcom/2005Convention.pdf, Accessed: 7/8/2006.

WIPO (1996a) *Copyright Treaty*, Adopted in Geneva on December 20, Available at: http://www.wipo.int/clea/docs/en/wo/wo033en.htm, Accessed: 18/08/2002.

WIPO (1996b) *Performances and Phonograms Treaty*, Adopted in Geneva on December 20, Available at: http://www.wipo.int/clea/docs/en/wo/wo034en.htm, Accessed: 18/08/2002.

Wolfke, K. (1993) *Custom in Present International Law*, Martinus Nijhoff Publishers, Dodrecht, Boston, London.

WSIS (2003) 'Declaration of principles', *Building the Information Society: A Global Challenge in the New Millennium*, 12 December, Available at: http://www.itu.int/wsis/docs/geneva/official/dop.html, Accessed: 31/3/2007.

Notes

[1]Section 3 of this paper is based on Polanski (2007, pp.337–345).

[2]Christophe G. v. Société France Télécom Interactive, *S.A.* [28.02.2001] JGT: 64/2001, RG: 00/106.

[3]http://www.marshal.com/trace/spam_statistics.asp, last visited: 7/04/2007.

[4]http://www.spamhaus.org/statistics/countries.lasso, last visited: 7/04/2007.

[5]http://www.spamhaus.org/statistics/spammers.lasso, last visited: 7/04/2007.

[6]http://www.irtf.org/charter?gtype=rg&group=asrg, last visited: 28/03/2007.

[7]http://en.wikipedia.org/wiki/Spamdexing, last visited: 28/03/2007.

[8]http://en.wikipedia.org/wiki/Google_bomb, last visited: 28/03/2007.

[9]http://chongqed.org/, last visited: 28/03/2007.

[10]http://en.wikipedia.org/wiki/Spamdexing, last visited: 28/03/2007.

[11]http://en.wikipedia.org/wiki/Link_farm, last visited: 28/03/2007.

[12]http://tool.motoricerca.info/spam-detector/, last visited: 28/03/2007.

[13]http://www.google.com/support/webmasters/bin/answer.py?answer=35769, last visited: 28/03/2007.

[14]http://help.yahoo.com/help/us/ysearch/indexing/indexing-14.html, last visited: 28/03/2007.

[15]http://www.cookiecentral.com/c_concept.htm, last visited: 28/03/2007.