03.14

2. Jahrgang
Mai 2014
Seiten 81–124

www.PinGdigital.de

PinG

Privacy in Germany

Datenschutz und Compliance

ESV ERICH SCHMIDT VERLAG

86118

Privacy in Germany Datenschutz und Compliance PinG 03.14 2. Jahrgang Seiten 81–124

Inhalt

Impressum

PinG Privacy in Germany
2. Jahrgang (2014)
Erscheinungsweise: 6 mal jährlich
www.PinGdigital.de

Herausgeber: RA Prof. Niko Härting
Redaktion: RA Prof. Niko Härting, Nils Hullen, LL.M. (Compliance), RA Dr. Niclas Krohm, Dr. Carlo Piltz, RA Sebastian Schulz (Compliance)

Schriftleitung:
Dr. Niclas Krohm / Dr. Carlo Piltz
Schriftleitung PinG
Erich Schmidt Verlag GmbH & Co. KG
Genthiner Str. 30 G, 10785 Berlin
Telefax: 0 30/25 00 85-305
E-Mail: PinG@ESVmedien.de

Verlag: Erich Schmidt Verlag GmbH & Co. KG
Genthiner Straße 30 G, 10785 Berlin
Telefon (0 30) 25 00 85-0, Telefax (0 30) 25 00 85-305
E-Mail: ESV@ESVmedien.de, Internet: www.ESV.info

Vertrieb: Erich Schmidt Verlag GmbH & Co. KG
Genthiner Straße 30 G, 10785 Berlin
Postfach 30 42 40, 10724 Berlin
Telefon (0 30) 25 00 85-229, Telefax (0 30) 25 00 85-275
E-Mail: Abo-Vertrieb@ESVmedien.de
Konto: Berliner Bank AG, Kto.-Nr. 512 203 101, BLZ 100 708 48
IBAN: DE 31 1007 0848 0512 2031 01
BIC(SWIFT): DEUTDEDB110

Bezugsbedingungen: Jahresabonnementpreis € 138,– (inkl. eJournal und Archiv); Einzelheft im Abonnement (6 x jährlich) € 23,–; Einzelheft € 25,–. Alle Preise jeweils einschl. Umsatzsteuer und zzgl. Versandkosten. Die Bezugsgebühr wird jährlich im Voraus erhoben. Abbestellungen sind mit einer Frist von 2 Monaten zum 1. 1. j. J. möglich.

Anzeigen: Erich Schmidt Verlag GmbH & Co. KG, Genthiner Straße 30 G, 10785 Berlin
Telefon (0 30) 25 00 85-629, Telefax (0 30) 25 00 85-630
E-Mail: Anzeigen@ESVmedien.de

Anzeigenleitung: Sibylle Böhler

Es gilt die Anzeigenpreisliste Nr. 2, vom 1. Januar 2014, die unter
http://www.esv.info/z/PinG/zeitschriften.html bereitsteht oder auf Wunsch zugesandt wird.

Manuskripte: Hinweise für die Abfassung von Beiträgen stehen Ihnen auch als PDF zur Verfügung unter: www.ESV.info/zeitschriften.html.
Von Text und Tabellen erbitten wir neben einem sauberen Ausdruck auf Papier – möglichst ohne handschriftliche Zusätze – das Manuskript auf CD-ROM oder per E-Mail bevorzugt in Word, sonst zusätzlich im RTF-Format. Zur Veröffentlichung angebotene Beiträge müssen frei sein von Rechten Dritter. Sollten sie auch an anderer Stelle zur Veröffentlichung oder gewerblichen Nutzung angeboten worden sein, muss dies angegeben werden. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag das ausschließliche Verlagsrecht und das Recht zur Herstellung von Sonderdrucken für die Zeit bis zum Ablauf des Urheberrechts. Das Verlagsrecht umfasst auch die Rechte, den Beitrag in fremde Sprachen zu übersetzen, Übersetzungen zu vervielfältigen und zu verbreiten sowie die Befugnis, den Beitrag bzw. Übersetzungen davon in Datenbanken einzuspeichern und auf elektronischem Wege zu verbreiten (online und / oder offline), das Recht zur weiteren Vervielfältigung und Verbreitung zu gewerblichen Zwecken im Wege eines fotomechanischen oder eines anderen Verfahrens sowie das Recht zur Lizenzvergabe.
Dem Autor verbleibt das Recht, nach Ablauf eines Jahres eine einfache Abdruckgenehmigung zu erteilen; sich ggf. hieraus ergebende Honorare stehen dem Autor zu. Bei Leserbriefen sowie bei angeforderten oder auch bei unaufgefordert eingereichten Manuskripten behält sich die Redaktion das Recht der Kürzung und Modifikation der Manuskripte ohne Rücksprache mit dem Autor vor.

Zitierweise: PinG Jahr, Seite

ISSN: 2197-1862

Satz: multitext, Berlin

Druck: Ludwig Austermeier, Offsetdruck, Berlin

Managing Partner at Dimitrov, Petrov & Co. Law Firm, Sofia, Bulgaria
Professor at the University for Library Studies and Information Technologies, Sofia, Bulgaria

Legality of spam filters and blacklists

Assoc. Prof. Dr. George G. Dimitrov

The wide penetration of Internet brought to life new realities unknown so far to society. One of these realities proves to be the use of Internet for sending billions of unsolicited communications known as "spam", at practically no cost. On the one hand, commercial communications serve as a base for the turnover and the development of e-commerce. On the other hand, however, these communications "eat" huge amounts of peoples" daytime resulting in shortening the usable time for generating effective gross domestic product. On a large scale, the damage to society is huge. Moreover, instead of increasing the turnover, the spam leads to damages to addressees due to the generated substantial traffic. To fight this new realm, lots of technological solutions came into life. Inter alia, these involve the usage of spam filters and blacklists. As the essay will show, the usage of these useful from practical point of view technologies proves to be on the edge of legality. They might reveal the secrecy of the communications and might seriously harm the bona fide users in their relations while using the Internet. The article will raise questions on the legality of these realms.

I. Introduction

The fast penetration of information technologies and particularly Internet brings into life new realms. In order to be more economically efficient, society constantly invents new ways to ease its life. Undoubtedly, using electronic messages is a great advantage to both the business and the social life of people. Positive inventions, however, many times come along with negative consequences. So along with wanted and, moreover, needed messages, on an everyday basis, email users receive billions of unsolicited communications.

On the Internet the word "spam" is used to address the junk communications, also known as "unsolicited commercial emails" (UCE). UCE is not only a nuisance but it is also an easy access point for viruses and malicious software. Spam is a constant problem for businesses and individuals. A survey made by the Bulgarian Law and Internet Foundation reads that if no spam filters were widely employed, more than 15% of the daytime of people would be dedicated to reading, identifying and deleting spam messages.[1] This would lead to the loss of the social potential to generate GDP. Moreover, the wide penetration of spam results in generating quite substantial Internet traffic to the detriment of Internet users. This is especially crucial where the Internet traffic is charged to the user per volume of the transferred data (data roaming, pay per use billing, etc.).

1 The Survey is available at www.netlaw.bg.

II. Spam filters

1. The Realm

In order to solve this problem, the Internet industry has developed a filtering solution known as "spam filters". These systems use a set of techniques to determine which of the incoming messages is spam. Several different types of spam filters are presently available and put into use: content filters, header filters, general blacklist filters, rules-based filters, permission filters, etc. All stated above use different criteria to perform filtering such as review of the message content or review of the email header, search for specific wording in the subject line or body, etc.

On the positive side, spam filters make Internet users' life easier by identifying unsolicited messages and thus storing them in another mailbox or deleting them. The process allows users to more easily dispose of unsolicited communication and in such a way saves them working and private time.

2. The Problems

The spam filtering system "reads" and processes the personal or business correspondence exchanged. Unfortunately, the system is not perfect. It does make mistakes. For example, if a message contains a few words that the spam filter acknowledges as UCE, the message will automatically be marked as unsolicited email and deprived of being delivered to the addressee. So the email is actually wanted but gets averted just because the system "reads" it wrong. The legal problems arising thereof are twofold.

a) Intervening in Legitimate Relations

More often than not, filtering systems are deployed and maintained by someone else – the internet society or communications services provider – the owner of the social network, the forum, the e-mail, or the mobile operator. Their systems often filter the communications even without the consent of the addressee. Although this process runs in an automated regime, behind the system always rests a real person – natural or legal, who owns it and who has access to and control of the filtered messages. By employing the spam-filtering technology such person may prevent solicited and legally binding statements from reaching their intended recipients and thus cause damages. Legally binding rights and obligations would not arise or might be affected.

b) Privacy Breach

By employing technologies which "read" and filter communications based on their content might seriously breach the security and confidentiality of correspondence. For example – based on three words "Viagra", "woman" and "sex" a message would be filtered by almost 40% of the spam filters employed worldwide. And what if a man sends a very sensitive private massage to his beloved that he has bought Viagra, so that they will have a sexual experience at home later tonight? Who has granted the right to someone to reveal the secrecy of personal messages? Are we all happy to have someone revealing the secrecy of our messages? The secrecy of the communications is proclaimed as a basic human right,[2] while in most countries it is established as a constitutional right.[3] Even more, the criminal laws criminalize the unlawful revealing of the contents of an electronic communication or intercepting or preventing messages of being delivered to the intended addressee.[4]

III. Blacklists

1. The Concept

Another technology used to fight the spam is the use of the so-called blacklists.

As per the common IT jargon the terms "blacklist" or "block list" are used to designate a specific control mechanism used to determine whether from a certain IP address unsolicited communications are being sent. Once determined as such, the traffic to and from such sources shall be restricted. This is achieved by entering the source into specially designated servers, who serve as centralised data storage where all addresses or domains are stored in databases designed for these purposes. Depending on the list type, the data is stored in tables containing information on when the address was blocked and why. The blocking can be implemented on local servers or the client could use global servers, which share their records through software or DNS (DNS stands for Domain Name System, not for Do Not Solicit) based system. For example, the most used type by mail servers is DNSBL (DNS-based Blackhole List), where the information is stored in databases on different servers with public addresses, so when a sender sends an email, the mail server of the recipient is making query to the DNSBL server. Depending on the DNSBL server's reply, the mail is allowed to pass through (if the sender address has a positive status) or gets blocked.

2. The Problems

Undoubtedly, blacklists help Internet users in the constant fight with the unsolicited communications and thus allow them to be

2 The Universal Declaration of Human Rights declares that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks (Art. 12). The same idea is also promulgated in the European Convention of Human Rights (Art. 8), the Charter of Fundamental Rights of the European Union (Art. 7).

3 In this sense see: Art. 34, Para. 1 of the Constitution of the Republic of Bulgaria; Art. 29, Para. 1 of the Constitution of the Kingdom of Belgium; Art. 19, Para. 1 of the Constitution of the Hellenic Republic; Section 10, Para. 1 of the Constitution of Finland; Art. 10, Para. 1 of the Basic Law for the Federal Republic of Germany Section 43 of the Constitution of the Republic of Estonia; Section 72 of the Constitutional Act of Denmark; Art. 5 of the Constitution of the Federative Republic of Brazil; Section 18 of the National Constitution of the Argentine Republic; Art. VI of the Fundamental Law of Hungary, Art. 15, Para. 1 of the Constitution of the Italian Republic; Art. 18 of the Constitution of the Republic of South Korea; Art. 23, Para. 2 of the Constitution of the Russian Federation; Art. 96 of the Constitution of the Republic of Latvia; Art. 22, Para. 2 of the Constitution of Lithuania; Art. 25 of the Political Constitution of the United Mexican States; Art. 13, Para. 1 of the Constitution of the Kingdom of the Netherlands; Art. 21 of the New Zealand Bill of Rights Act; Art. III, Section 3, Para. 1 of the Constitution of the Republic of the Philippines; Art. 28 of the Constitution of Romania; Art. 34, Para. 1 of the Constitution of the Portuguese Republic; Art. 41, Para. 1 of the Constitution of the Republic of Serbia; Art. 40, Para. 1 of the of the People's Republic of China; Section 14 of the Constitution of the Republic of South Africa, etc. In some cases even though not explicitly stated in the basic law, the secrecy of communication, respectively – correspondence is acknowledged by national (supreme) courts as a constitutional right derivative from the inalienable human rights promulgated in the respective constitutional act or in international agreements adopted into national laws – i. e., the United States of America; the United Kingdom; the Republic of India; the Republic of France etc.

4 See: Art. 171 of the Bulgarian Criminal Code reads that anyone who unlawfully comes to know an electronic communication, which is not addressed to them or averts such message from its addressee, shall be punished with imprisonment; Section 202 of the Criminal Code of the Federal Republic of Germany states that whoever, without authorization: opens a sealed letter or another sealed document that was not intended to come to his attention or obtains knowledge of the content of such a document without opening the seal by using technical means, shall be punished with imprisonment for not more than one year or a fine if the act is not punishable under Section 206; Art. 138, Para. 1 of the Penal Code of the Russian Federation states that violation of the secrecy of correspondence, telephone conversations, or postal, telegraphic, or other messages of individuals, shall be punishable by a fine in the amount of 50 to 100 minimum wages, or salaries or in the amount of the wage or salary, or any other income of the convicted person for a period of up to one month, or by obligatory works for a period of 120 to 180 hours, or by corrective labour for a term of up to one year; Art. 226–15 of the Penal Code of the Republic of France, reads that maliciously opening, destroying, delaying or diverting of correspondence sent to a third party, whether or not it arrives at its destination, or fraudulently gaining knowledge of it, is punished by one year's imprisonment and a fine of € 45,000. The same penalty applies to the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by means of telecommunication, or the setting up of a device designed to produce such interceptions; Art. 184, Para. 1 of the Canadian Criminal Code reads that every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; Art. 157, Para. 1 of the Estonian Penal Code states that violation of the confidentiality of a message communicated by a letter or other means of communication is punishable by a pecuniary punishment; Art. 212, Para. 1 of the Romanian Penal Code states that the act of opening postal communications addressed to another person or listening to a communication by telephone, telegraph or by other means of remote transmission without right, shall be punished by strict imprisonment from one to 3 years or by days/fine; etc.

more efficient in their work or personal life. However, several serious legal vulnerabilities affecting legitimate rights and interests of the internet users could be identified.

a) Restraining of Receiving Solicited Correspondence

The distinction between solicited and unsolicited communications is blurred. In some cases most or even all legitimate emails never get delivered because the IP address is on a blacklist along with a known "spammer". A company's or a person's e-mail server IP address is blocked just because one or another user of the e-mail service proves to be a spammer. The block of an IP address may result in hampering the usage of many domains hosted on the server with the blocked IP address. The process depends on the service and provider since each organization which offers DNSBL, RBL or similar services, has its own policy for listing addresses or domains. If the respective address (IP or domain name) appears in a blacklist, usually it is because it has been reported by a client (via software developed for automation/manual reporting) or by some ISP. The blacklisting may occur because it has been determined that someone in the respective network is sending spam or malicious content. Most of blacklist providers rely on rating systems which add or remove ratings to addresses or domains that exist in their databases. For example, each time a specific address or domain gets reported, the rating increases by some value. If the total value goes above the limit set by the provider, the address or domain is marked as spam or a dangerous sender and it is then being moved to the blacklist.

The DNS-based anti-spam databases are used by most ISPs. Their webservers usually check the lists for IP addresses linked to information systems, which send out spam or perform other unsolicited activity. If the activity is identified as such, the IP addresses may become listed in other databases, simply because it has been blacklisted in one of them.

The aftermath of this is that every email, every user account is being blocked – no incoming or outgoing correspondence is allowed. So many *bona fides* persons might be restrained from receiving their correspondence (whether personal or business) just because someone has created and avertedly used an account for spamming purposes.

b) Harm of Legitimate Interests

Getting solicited emails averted could further seriously harm business relationships. The result is lack of communication with business partners, getting transactions cancelled because of delay in payment, missing deadlines, omission of notification to create, change or cancel a reservation for a business meeting, travel, loss of contacts, lost profits, untimely solved problems, slow logistics operations leading to a progressive accumulation of errors which in turn leads to the loss of money, customers, vendors, partners, etc.

Unfortunately, I could speak from personal experience. A few years ago the mailboxes under our law firm domain @dpc.bg were served by an email server, which was operating mailboxes of another domain – @lex.bg. At this second domain, everyone was allowed to register and use free email service. Thus, one of the users used the service for sending thousands of unsolicited communications resulting in the IP address of lex. bg blacklisted. The mail service of our law firm also stopped – we were put in a situation where we lost lots of money because of being deprived of fulfilling obligations towards our clients, many were affected of delayed documents and maturity terms expired. As one could imagine, we were quite unhappy and although we put all efforts in explaining and taking the IP address of the mail server out of the blacklists, the situation continued for a few weeks. The IP address was taken off the last blacklist after three months. Needless to say, no person or entity shall be able to prevent with impunity third parties from fulfilling their contractual obligations. Unfortunately, this is exactly one of the blacklisting side effects. The blacklisting may result in triggering civil liability of the blacklist service providers.[5] But similarly to the legal effects of the spam filters, the use of blacklists may also result in criminal liability – no one is allowed to avert or prevent from receiving other persons' communications without their consent – the secrecy and privacy of people's personal lives including their right of free and confidential correspondence shall be infringed.[6]

IV. Conclusion

In conclusion, it should be pointed out that undoubtedly spam filters and blacklists are useful technological instruments to Internet users in their fight against unsolicited communications. These filtering systems, however, have a full and often unrestricted access to user's correspondence.

Considering the above said, however, it becomes evident that both spam filters and blacklists are not a panacea to fight the spam, on the contrary – they might hamper seriously the secrecy of the communications and hence, the private life of people, thus standing on the verge of the legality. When employing filtering instruments, it should be always with the consent and the clear knowledge of the parties to the communication services, which

5 The obligation for third parties to restrain from impeding parties' performance due to contract may be based on the general liability clause not to cause damages to others which exists in most legal systems with regards to contractual obligations. Furthermore in some Roman-law countries that rule is recognized through the principle of the opposability of the contract: in France the possibility of invoking the contract against third parties, which has been expressly recognised by the *Cour de cassation* as a general principle of law, meaning that third parties must respect the situation that the contracting parties wanted to establish. In this way, the opposability of the contractual situation against third parties appears as the necessary compliment to the binding force of contract. The contract would run the risk of being deprived of all efficacy if third parties were able to ignore or abuse at their whim the situation created by the contract; in Spanish law, third parties must respect the legal situation which the contract gives rise to. This requires them, if they are aware, to not create any ties with a party to the contract which could lead to the performance of the contract becoming difficult or even impossible; in Italian law, although the effect of the contract is envisaged from the angle of binding force, and therefore only affects third parties in the specific cases laid down by statute, it is nonetheless recognised that third parties should not endanger the performance of the contract. In the USA the issue arising from situation in which a party believes it has been wrongfully included in a spam filter or block list and therefore has been damaged, is usually resolved on the basis of claims covering defamation and intentional interference with prospective business relationships. The defamation action is usually founded on the fact that that apart from being viewed as a negative activity, spamming is a crime in a number of jurisdictions. In accordance to the general principles of common law, publishing an accusation of a crime or a statement which damages the subject's ability to do its business is actionable per se without need to show special damages. On the other hand the intentional interference with prospective business relationships claim may be based on the tort stating that one who intentionally and improperly interferes with another's prospective contractual relation (except a contract to marry) is subject to liability to the other for the pecuniary harm resulting from loss of the benefits of the relation, whether the interference consists of (a) inducing or otherwise causing a third person not to enter into or continue the prospective relation or (b) preventing the other from acquiring or continuing the prospective relation. Apart from the above with regard to the specifics of the case and the applicable law, claims may be founded on unfair competition or restraint of trade.

6 See notes 2–4, *supra*.

can be hardly achieved in cases where no contractual relationship could be established between the service provider and the sender or the addressee of the communication.

When elaborating new technological control mechanisms to deal with one realm, the practical aspects shall not prevail over the legal ones. The legality of spam filters and blacklists must be in accordance with the secrecy and confidentiality of correspondence, which proves to be hardly achieved.

PRIVACY NEWS

The Australian Privacy law reform – what has changed?

Dr. Jonas Kahl, LL. M.

On 12 March 2014, the new Australian Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Privacy Amendment Act) came into effect. It is the result of a reform discussion started in 2004 and makes a number of significant changes to the former Privacy Act 1988 (Privacy Act), particularly with the collection of information online. The Privacy Act still exists and includes the changes of the Privacy Amendment Act now. In the following the most important changes of this reform are emphasised, after a short historical review.[1]

I. History of the Australian Privacy Act

Initially the primary Privacy Act from 1988 had the objective to protect only personal information which was in the possession of governmental agencies. For this purpose it was based on eleven so called "Information Privacy Principles" (IPPs). These were based again on OECD guidelines and set out standards relating to collecting, storing, using and disclosing, providing access to, and correcting personal information.

Additionally in 1991, regulations were introduced for the handling of consumer credits and in 2001 the coverage was extended to some private sector organisations. In 2010, the Office of the Australian Information Commissioner (OAIC) was established, which is headed by the Australian Information Commissioner. Referring to the Australian Information Commissioner Act 2010 (AIC Act), the OAIC is responsible for all questions of freedom of information functions, privacy functions and information policy functions.

II. Changes resulting from the reform

The major reform of privacy law is the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Privacy Amendment Act) which commenced in March 2014. It introduced many significant changes to the Privacy Act, revising the privacy principles and introducing new credit reporting laws, providing External dispute resolution (EDR) schemes and civil penalties.

Dr. Jonas Kahl, LL.M. studierte Rechtswissenschaft in Leipzig, Rom und Mainz mit Schwerpunkt im Medien- und IP-Recht. Sein Referendariat absolvierte er in Berlin und verbrachte seine Wahlstation bei der IP- und IT-Rechtskanzlei FAL Lawyers in Melbourne.

III. Australian Privacy Principles (APPs)

Most important are the changes of the Principles in Schedule 1 of the Act. Here the former "Information Privacy Principles" (IPPs) were replaced by the "Australian Privacy Principles" (APPs).[2] In comparison with the IPPs only a part of the APPs remained similar or same.

The object of the new APPs is to ensure that governmental agencies and some pri-

1 Thanks to Marianne Dunham from FAL Lawyers (fal-lawyers.com.au) for suggestions.

2 Australian Privacy Principles, available at http://www.comlaw.gov.au/Details/C2014C00076/Html/Text#_Toc382303234.