THE SPAM ISSUE IN MOBILE BUSINESS
A COMPARATIVE REGULATORY OVERVIEW

Giovanni Camponovo, Davide Cerutti
The University of Lausanne
Giovanni.Camponovo@hec.unil.ch, Davide.Cerutti@idj.unil.ch

ABSTRACT

The emerging mobile industry is expected to be characterized by increasingly personalized and location-based services. Among these services, personalized mobile marketing and advertisement services are predicted to be particularly important. However, besides the excitement about the potential innovative one-to-one marketing strategies enabled by the mobile medium, growing concerns are being raised about the protection of the users’ privacy from what can become extremely intrusive practices in an intimate personal space. There is indeed a thin line between providing useful services and bombarding the user with mobile spam. Conscious of the importance of solving this sensible issue, the mobile marketing association itself has issued privacy guidelines to its members. However, because this self-regulation has proven weak in protecting users from abuses, regulatory bodies throughout the world have issued laws to protect user privacy. This paper illustrates and compares the regulatory frameworks of Switzerland, the European Union and the United States, and analyzes their likely implications for the mobile business industry.

KEYWORDS

Mobile spam, unsolicited advertising, legal aspects, privacy, data protection
1. INTRODUCTION

The emerging mobile business industry is characterized by a multiplicity of technologies which potentially enable a massive amount of innovative services. According to the industry’s conventional wisdom, future mobile services will be increasingly customized to each individual user and its usage context. This can be done by taking into account a mixture of personal information, physical location and other contextual data. The intimate personal nature of mobile devices and the availability of location and contextual information are indeed frequently referred to as the most valuable unique characteristics and influential drivers of future mobile business services (Müller-Veerse 2000; Keen et al. 2001; May 2001). Location-based services are considered a killer application of mobile computing (Oertel, Steinmüller et al. 2002). Some empirical evidence confirms that personalization is indeed perceived among users as a major factor for service provider selection (Ho et al. 2002).

Among these services, particular attention has been devoted to mobile marketing, which has been predicted to be among the most successful mobile commerce applications and a key provider of m-commerce revenues (Müller-Veerse 2000). Mobile marketing broadly refers to the distribution of any kind of promotional or advertising messages to customer through wireless networks (Kalakota et al. 2002). From a marketing point of view, the mobile communications medium has highly valuable peculiarities which the marketing industry will be eager to exploit, especially as a complement to the traditional marketing channels. Mobile devices have indeed shown to be very intimate personal devices which provide marketers with unrivalled mass customization and one-to-one marketing capabilities combined with large reach, low costs, instantaneous feedback, 24h reachability and localization contextualization possibilities (Huisken et al. 2001). The combination of all these factors creates what has been described as the dream environment of every marketer (Müller-Veerse 2000). It is expected that mobile advertisement will be highly personalized and location-based.

Despite the excitement about potential benefits of the innovative marketing strategies enabled by the mobile medium, several issues must be resolved before this potential can realize (Tarasewich et al. 2002). Among them, protection of user privacy may be considered one of the most critical for end user adoption of mobile services. The emergence of personalized and location-based services has indeed paved the way for what, unless carefully monitored, can become extremely intrusive practices and jeopardize the privacy of mobile users' personal data (Giaglis et al. 2003).

In particular, the emerging phenomenon of mobile spam caused by unsolicited mobile messages or advertisements is becoming a major nuisance for users. For instance many cases of unsolicited messages which dupe people into phoning premium rate numbers have recently been reported and generated a growing number of complaints to regulatory authorities (cf. Icstis 2002). Unlike the email spam problem, the issue is not one of scale - mobile spam is unlikely to reach the overwhelming proportions of email spam because SMS is not free - but of sensitivity as the mobile phone is perceived as an extremely personal device and rarely leaves our side (Clark 2004).

Besides worries about intrusion in one’s private space, mobile spam raises privacy concerns related to the utilization of personal and location information used to craft customized advertising messages. Information privacy concerns have recently been a major issue as users become aware of the electronic prints they leave and the amount of information that can be collected and assembled about them (Cranor 1999). This is especially true in mobile business where mobile operators can easily assemble detailed user profiles as they can easily identify users and access their demographic data, location information, accessed services and calling patterns (Müller-Veerse 2000), thereby raising significant
privacy and "big brother" concerns (Kaasinen 2003). The problem is that these concerns are most likely to cause users to not adopt services that they will otherwise be likely to use. It has indeed shown that privacy concerns negatively affect the choice of service operator and the adoption of personalized mobile services (Ho et al. 2002).

These concerns call for industry players and regulation authorities to conceive and actuate effective measures to alleviate these problems. The most challenging aspects in designing these solutions is to reconcile users’ demand for highly personalized services with their desire for privacy (Sadeh 2002). It is in the self-interest of the industry to adopt self-regulation practices as public intervention is likely to be heavier if these turn out to be ineffective.

Privacy concerns can thus be limited by various organizational, technological, social and legal means. While all of them are important to attenuate the problem, the objective of this paper is to provide an overview of the legal solutions which are in place for protecting the user’s privacy and personal data. In particular, the paper is focused on the illustration and comparison of the regulatory frameworks of Switzerland, European Union and the United States.

The paper is structured as follows. The next section explains what the privacy issue is and illustrates the two main principles underlying it: restricted access and control. Section 3 illustrates how the privacy issue relates to mobile business, with a particular attention to the spam problem. Section 4 provides an overview of the legal measures proposed by the regulatory framework in Switzerland, European Union and the United States. Finally, section 5 illustrates the most important elements that can be derived from these legislations and with a critical assessment of their effectiveness.

2. THE PRIVACY ISSUE

2.1 The notion of privacy

The need for privacy stems from our notion of individualism and the sovereignty of our own person: because we feel responsible for our actions, it is necessary for us to maintain control on our decisions and actions (Vogt 2002). When we allow others to interfere with our personal space or access personal information about us, this potentially harms us and diminishes the control we have over our own lives. It is therefore important for us to be able to protect that space against unwanted intrusions.

As social beings, however, we must accept some amount of disclosure in order to interact with one another socially. The amount of disclosure to other people we are willing to accept depends on several factors such as how sensitive the information is considered, expectations as how information will be used, how familiar the person is with the entity collecting the information, its trust and reputation, and what compensation or benefits are being offered to the person in exchange for the information (Vidmar et al. 1985; Goodwin 1991; Sheehan et al. 2000; Olivero et al. 2004).

For these reasons, it is important for us to be able to both restrict access to our personal space and information so as to being protected against intrusions in it as well as to control the conditions of its selective disclosure to other people. Accordingly, the concepts of restricted access and control have been at the core of privacy definitions in the literature.

The concept of privacy of information has indeed traditionally been defined in terms of control over the divulgence of sensible information about one's private life. In this respect privacy is seen as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent
information about them is communicated to others” (Westin 1967, p7). Similarly, it has been observed that “the basic attribute of an effective right of privacy is the individual’s ability to control the circulation of information relating to him” (Miller 1971, p25).

Tavani and Moor (2001) argue that although the notions of privacy and control naturally fit together, they should be treated as separate mutually reinforcing elements. In their view, “the concept of privacy itself is best defined in terms of restricted access, not control. Privacy is fundamentally about protection from intrusion and information gathering by others. [...] Sensitive personal information ought to be private even if its owner is not in a position to control it”. On the other hand, they recognize that control of personal information plays an essential role in the management of privacy and justifies the framing of suitable privacy policies.

Intended as the protection from unwanted intrusion in and information gathering about one’s private life, privacy is widely recognized as a universal right. The Universal Declaration of Human Rights states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”\(^1\). Accordingly, virtually all societies establish normatively private situations, zones of privacy, which limit access to people or aspects about them under certain conditions (Moore 1984).

Nevertheless, as we will see in section four, the boundaries of these zones and the conditions of access to them are much more difficult to establish as “any person who chooses to live in a community must accept the restraints and intrusions upon her life occasioned by the social organization necessary to enable the community to function effectively” (Lyford 1994). The limits of privacy depend therefore on what the legitimate interests of society and individuals are considered to be and consequently vary somewhat across cultures and along the evolution of society.

3 Privacy concerns in mobile business

Privacy concerns have presumably always existed to some extent in the history of mankind. Yet, this issue has recently gained unprecedented attention with the advent and widespread adoption of information and communication technologies and in particular the Internet. Users have essentially become involved since the massive adoption of the Web and the subsequent flurry of media reports about cookies and web sites tracking activities. Since then, users have begun to realize the amount of electronic prints they leave and the consequent bulk of information that can potentially be gathered about them. It is not only what a single site can collect to raise concerns, but rather the aggregation of all these sources and especially their association with personal data about the user.

These concerns are well-founded given that, due to rapid advances in data collection and processing technologies, organizations have extraordinary capabilities to efficiently collect, store, analyze and exchange a vast amount of personal data. Nevertheless, aside from many complaints about unwanted junk mail, there have been few allegations of actual online privacy violations so far (Cranor 1999).

With the arrival of mobile data networks, the privacy issue is even more salient. A number of important new concerns add to the current ones, mainly stemming from the fact that mobile devices are intimately personal and are always with the user. Four major concerns can be identified: mobile

\(^1\) Art. 12 of the Universal Declaration of Human Rights, United Nations, 1948.
Mobile spam is a particularly annoying problem. Spam itself is a problem for many reasons: privacy, deception of consumers, protection of minors and human dignity, extra costs for businesses, lost productivity. More generally, it undermines consumer confidence, which is a prerequisite for the success of e-commerce, e-services and, indeed, for the Information Society (Commission of the European Communities 2004). Unlike the email spam problem, however, the issue is not one of scale - mobile spam is unlikely to reach the overwhelming proportions of email because messaging is not free - but of sensitivity, as the mobile phone is perceived as an extremely personal device and rarely leaves our side (Clark 2004). Unwanted SMS messages can bother the user at any moment and in a variety of contexts (email spam is limited to when reading emails). For that reason, mobile spam is considered an intrusion in a very intimate personal space. Moreover, due to mobile devices limitations, advertising messages may impede the reception of regular messages and require more effort to delete.

The personal identification problem deals with the fact that mobile devices are very personal and are always with us. Network operators can easily identify the user as they authenticate in the network (e.g. using SIM information) and get the corresponding demographic information. Mobile operators need to collect personal information for billing their service to post-paid users, but are also required by law about their customers at the moment of contract subscription in order to prevent abuses from pre-paid users. Therefore, all what a user does with his mobile phone can easily be related to its person.

Mobile devices provide network operators the unique possibility to track the users’ locations anytime, anywhere. This raises the question of the right to locate a person and the use this information to provide location-based services. This concern is growing with the deployment of improved location technology: by using and combining triangulation techniques such as TDOA, OTD, AOA and TOA, users can be located with a fairly high precision of some ten to hundreds of meters depending on the density of antennas. Whether deployed to comply with regulation such as in the US (to support advanced emergency services) or allow location based services, carriers are looking for commercial applications to offset their costs and may want to sell this information to third parties.

Finally, there may be concerns with the interception of wireless communications as radio transmission is by nature more susceptible to eavesdropping. Cellular networks such as GSM and GPRS appear to be reasonably secure against interception on the wireless link: calls are protected by symmetric encryption based on a shared secret key stored in the SIM module and the operator's authentication center. They do not however provide end-to-end security due to unsecured transmission between bases stations and on the wired part of the network (Lee et al. 1999). Still, the equipment and knowledge necessary to intercept these communications is rather exclusive. Wireless data networks such as Bluetooth and Wireless LANs seem to be much more vulnerable, especially when using the default equipment configuration. Emblematic are the well known security problems of the 802.11 WEP security protocol (Borisov et al. 2001; Housley et al. 2003) as well as the recent admission by Nokia of the possibility of stealing data from its Bluetooth-enabled devices (Nokia 2004).

In parallel to the awareness of information privacy threats, however, users have become aware of the value of personal information and seem disposed to reveal it in exchange of some form of benefit. Users have indeed reported willingness to disclose personal information when the perceived benefits associated with disclosure offset the higher risks of vulnerability (Goodwin 1991; Sheehan et al. 2000; Olivero et al. 2004). If the benefits - pragmatically evaluated in terms of the potential for improved services, more adapted information or even financial rewards - are perceived as large enough, some degree of privacy loss will probably be accepted.
In the mobile business industry, this makes a case for personalized and location-based services. For instance there is preliminary evidence that users are willing to accept to allow the use of location information to get useful location based services despite their worries about privacy and "big brother" concerns (Kaasinen 2003). This has also been confirmed by an empirical study which found that the higher benefits of personalization more that compensate the users privacy concerns (Ho et al. 2002).

An interesting application field where these concerns are especially salient is the mobile marketing industry. Prominent players in this field realized quickly that their brands would suffer if consumers believe their privacy is being violated. Conscious of the importance of solving this sensible issue, the Mobile Marketing Association itself has issued privacy recommendations to its members, recognizing that "failure to respond effectively to privacy issues and risks can result in adverse consequences that range from outright market rejection to regulatory enforcement action" (Mobile Marketing Association 2003). On the other hand, marketers advocate that by accurately targeting the messages to the right users by employing advanced personalization techniques and giving them some form of compensation, users would perceive these messages as useful and not as spam. Still, it can be argued that "there is a fine line between presenting consumers with useful services that are relevant to their location and preferences, and bombarding them with annoying location-sensitive ads" (Sadeh 2002).

Protecting privacy must be undertaken in combination with a number of other efforts. Legislations is the basis for privacy protection, but social norms, business practices and technical means can also contribute to this goal (Ackerman et al. 2001). According to (Wang et al. 1998), there are three main parties involved, each playing different roles: governments, businesses and individuals. Governments are principally responsible for promoting privacy laws and establishing independent privacy commissions to oversee the implementation of these laws. Businesses might promote self-regulation practices that overcome user concerns and foster market adoption. Finally, individuals are ultimately responsible for make an informed choice between the benefits of disclosing personal information and its associated risks. Moreover, they may also adopt privacy enhancing technologies, such as network and information security tools, although their effectiveness is yet to be proven (cf. Tavani et al. 2001) and they comport the risk of being suspected of practicing dubious activities.

While these different topics deserve an equitable attention, the focus of this paper is on the regulatory frameworks which are being deployed for protecting user privacy. In the following section, we will expose the regulatory framework of Switzerland, European Union and the United States.

3. COMPARATIVE EVALUATION OF REGULATORY FRAMEWORKS

General Principles

As illustrated by the preceding paragraphs, the key challenge in defining policies for protecting privacy is that the privacy rights of individuals should be balanced with the benefits associated with the free flow of information. There are a number of trade off between privacy and other matters among which the information needs of marketers and the consequent expectations for service levels which are only available if some personal information can be used (Goodwin 1991). The different frameworks all come up with their own measures which try to balance these contrasting interests.
In the considered regulatory frameworks - United States\(^2\), European Union\(^3\) and Switzerland\(^4\) - advertising is guaranteed by legislation. Advertising essentially is the communication of non-personal information with the purpose of persuading recipients to buy certain products or services or enhance the sender's image. It is considered to perform an important function in our economy, as it provides consumers with the information that they need to make decisions in the marketplace, and shall therefore be protected. It is a matter of public interest that private economic decisions are well-informed. To this end, the free flow of commercial information is indispensable.

In some circumstances, however, advertising can have perverse effects and must therefore be limited by regulation. It is for instance the case of unethical, political or aggressive advertising. This article is principally concerned in the aggressive advertising practices enabled by information and communication technologies. Technological development has indeed opened new ways for spreading advertisement messages: computer networks such as the Internet and mobile telephony are among the most important of these vehicles as they allow very easily to send a huge mass of messages to targeted individuals at virtually no cost. Because of this characteristic, advertisement on these media is today at the centre of the attention and widely debated, above all because of the overwhelming proportions taken by the phenomenon of spam. This technique can be conceived as a particularly aggressive form of advertisement, for it addresses personally to recipient and invades his personal space without his previous consent.

According to the restricted access principle exposed in section 2, the different legislations envision very restrictive conditions for allowing unauthorized access to the user personal data. On the other hand, according to the control principle, they provide the user with the faculty to choose to lessen the protection of its privacy.

Recent policy discussion has been framed around a set of core principles which shall guide development of privacy policies: notice or communication (users should be informed about the applied information practices), choice or consent (user should have the opportunity to decide and consent about the disclosure of personal information for the proposed conditions of use), access (users should be able to access information stored about them), security (data collectors should grant security and integrity of the collected information) and redress (enforcement mechanisms should exist to enforce compliance) (Goodwin 1991).

Among these principles, particular attention shall be given to granting user the faculty to choose about the disclosure of personal information. In fact, communication can be considered as instrumental in allowing user to make an informed choice, while security and redress can be thought as means to ensure that the choice of the user will be respected.

Discussion about information privacy has traditionally been centred around various mechanisms to provide users the possibility to express their informed consent to give up their privacy, be it for

---

\(^2\) The Supreme Court decided to accord First Amendment protection to commercial speech, including advertising, in the Virginia State Board of Pharmacy case.


\(^4\) Arrêts du Tribunal Fédéral Suisse (i.e. decision of the Federal Court of Switzerland, hereafter referred as ATF) ATF 120 Ib 142, March 11 1994; ATF 123 II 402, August 20 1997; ATF 123 IV 211, November 7 1997.
allowing use of personal information (e.g. for personalized or location-based services) or allowing
sending of unsolicited messages (e.g. advertisements).

In the case of mobile spam, two basic mechanisms are envisioned for allowing users to express their
choice whether they want to receive these unsolicited messages. In an opt-in system an individual has
to explicitly agree to receive such messages before the sender is allowed to send them, whereas in an
opt-out system these messages are considered to be legal unless the recipient explicitly opposes to
such messages. While the former is perfectly consistent with the fair information consent requirement,
whereas in the latter the individual has to disagree with its opposite and must reassert the principle
itself, individually and repeatedly (Regann 2003). Notice that, consistently with the opt-in principle,
the mere fact that mobile telephone numbers are publicly available, e.g. in telephone listings or on the
Internet, is not sufficient to constitute a right to use them freely5.

**The notion of spam**

Spam can be defined as unsolicited personal commercial communications, in particular those made
through electronic messages and to a massive number of recipients. Spam is therefore characterized by
the following properties:

- **Electronic.** An electronic communication is considered to be any communication conveyed through
electronic communications networks: “transmission systems […] which permit the conveyance of
signals by wire, by radio, by optical or by other electromagnetic means, including satellite
networks, fixed […] and mobile terrestrial networks, electricity cable systems […] networks used
for radio and television broadcasting, and cable television networks, irrespective of the type of
information conveyed6. These networks clearly encompass the Internet and mobile telephony
networks. Therefore, communications made through email and SMS are considered electronic and
may constitute spam. Also notice that the mode of the communication is irrelevant: of course most
of spam is in text form, but audio and video messages are equally concerned.

- **Unsolicited.** The transmission of advertising or informative material happens in the majority of
cases without the agreement of the addressee: he is most likely to be completely unaware that his
personal data is used for these purposes. The core and irrefutable principle underlying privacy
protection is that the addressee must express his informed consent to allow these uses of its
information. The debate is opened on the technique to adopt to collect that consent: opt-in or opt-
out. In an opt-in system the consent to receive such messages must be explicit before the sender is
allowed to send them, whereas in an opt-out system the consent is implicit and messages are
considered to be legal unless the recipient explicitly opposes to such messages. Obviously,
marketers prefer the opt-out because they can send messages until the addressee does not oppose,
whereas users favour the opt-in as they would not be unduly disturbed. A range of hybrid solution
are conceivable. A pragmatic compromise might allow a first contact asking the consent to send
future messages (Verbiest 2003) even tough users might be submerged by these first undesired
communications and raises the problem of whether the absence of response must be considered an

---

5 Cf. decision of the "Garante della privacy italiano" (i.e. Italian Privacy Commissioner) of January 11 2001,

on a common regulatory framework for electronic communications networks and services (Framework
Directive)
implicit consent or an implicit dissent (which in our opinion should be considered as an implicit dissent as it would otherwise be equivalent to an opt-out scheme). One further consideration about the usual mechanism to collect this consent, which is through web sites where the mobile phone number can be registered together with the possibility to indicate the objection to secondary uses of this number (e.g. in a checkbox). The simple fact to provide the telephone number let the consent to be presumed. In a more stringent view, however, it would be preferable to require the user to click on a box indicating the explicit consent.

- **Commercial.** Spam is typically characterized as communications with a commercial content or purpose. Of course, it is true that most of spam messages have an advertising or commercial nature and privacy policies tend to explicitly focus on commercial messages. Nevertheless, there are many non commercial messages that share the same annoyance characteristics and deserve to be considered as spam (Sorkin 2001). The distinction between commercial and non commercial messages is purely theoretical as nothing justifies a diversified treatment of these two types. Both types should therefore be treated as spam.

- **Mass communication.** Unsolicited messages are commonly considered as spam when they are sent to a critical mass of users. Yet, the question is how can this number of users to be set? Obviously any quantification is arbitrary. This number should take into account the memory and other capabilities of the receiving devices and, consequently, might well be much inferior for SMS than for emails. This number should not be excessively large and, in some circumstances, even a single unsolicited contact might be taken for spam (Sorkin 2001 p327).

- **Personal.** Even tough this characteristic is seldom mentioned, one central characteristic of spamming is that messages are personally directed towards a number of users. This permits to exclude messages conveyed through the mass media. For instance European legislation excludes “information conveyed as part of a broadcasting service to the public except to the extent that the information can be related to the identifiable subscriber or user receiving the information”.

**The European Union**

The European legislation has experienced an interesting evolution in the recent years. Early partisan of the opt-out system, legislation has experienced a transition towards the opt-in approach passing

---

7 The European and Swiss regulatory frameworks essentially focus on commercial spamming. In the US, the distinction between commercial and non commercial spam is not pointless in the light of the First Amendment. For a consideration about the relationship between spamming and the First Amendment see Cyber Promotion vs. AOL, November 4 1996, http://www.jus.unit.it. Tough, the CAN-SPAM act refers to commercial e-mails.

8 For instance, Ontario Inc. vs. Nexx Ondine Inc., Ontario Supreme Court, September 7 1999: more than 200'000 emails per day; State vs. Heckel, US Supreme Court, September 18 2001: Heckel sent between 100'000 and 1’000’000 advertising emails per week and sold between 30 and 50 products per month.

through an intermediate stage in which opt-in was envisioned for some particular cases\textsuperscript{10}.

The current European legislation about spamming consists in two principal directives: the Directive on electronic commerce\textsuperscript{11} and the Directive on privacy and electronic communications\textsuperscript{12}. They define spam as unsolicited commercial communications. Communications mean “any information exchanged or conveyed […] by means of a publicly available electronic communications service” except information conveyed as part of a broadcasting service to the public to the extent that it is not related to an identifiable user\textsuperscript{13}. Commercial nature is intended 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”\textsuperscript{14}.

The current legislation has adopted the principle of opt-in as “direct marketing may only be allowed in respect of subscribers who have given their prior consent”\textsuperscript{15}. Even though SMS are not explicitly mentioned, they must nevertheless be considered in view of a teleological interpretation of the norm (Vebriest 2003 p1, Carpentier p9), considering that the protection of individuals “must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention”\textsuperscript{16}. The norm can thus be easily extended to include new communication means as needed.

The reason underlying the opt-in choice is to avoid users to be submerged by an excessive amount of messages since it is easy and inexpensive to send massive amounts of electronic advertising messages.

To this principle, however, follows the exception of a pre-existing commercial relationship which envision the opt-out system: "where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use”\textsuperscript{17}. It is worth pointing out that only the company involved in the commercial relationship obtains this right, which cannot be transmitted to other parties. Moreover, while this opportunity is limited to similar products or services, what must be considered as similar is subject to interpretation (Vebriest 2003 p2).


\textsuperscript{12} Directive on privacy and electronic communications

\textsuperscript{13} Art. 2 lit. d of the Directive on privacy and electronic communications

\textsuperscript{14} Art. 2 lit. f of the Directive on electronic commerce

\textsuperscript{15} Art. 13/1 of the Directive on privacy and electronic communications

\textsuperscript{16} § 27 of the 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 (Directive on data protection):

\textsuperscript{17} Art. 13/2 of the Directive on privacy and electronic communications
A bunch of other exceptions are also envisioned so as to avoid the negative effects of an excessive protection and maintain a balance with the legitimate interests of other parties. Use of personal data is thus lawful when it is "necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding" as well as "in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies".

From the viewpoint of this legislation, mobile services such as location-based services, mobile advertising and push information services should be allowed only with the previous and explicit consent of the user and the user should be given a free and easy way to block these messages.

In addition to the legislation contained in the directives, there are a few judgments by the various Member States courts on cases involving mobile spam through SMS. These judgments illustrate the narrow relationship between advertising and various juridical domains.

An Austrian court judged the case of a company sending SMS indicating that the recipient has won a prize and must call a number to claim it. According to the judges, these messages are considered as spam for two reasons. Firstly, these messages are illicit according to the opt-in principle as they are unsolicited advertising messages sent without the previous consent of the receivers. Secondly, they are a particularly aggressive form of advertising and constitute a serious annoyance to users as they are taken by surprise and do not have enough time to meaningfully consider the proposal. Moreover, the court considers this practice as unlawful in view of the unlawful competition law.

A German court judged the case of users who subscribed on a portal to a service for sending free SMS. The portal subsequently communicated the personal data of the user to a third party which sent the contested advertising messages. The court established that this practice was unlawful as the transmission of advertising messages without the previous consent of the recipient is considered a privacy violation for private users. More interestingly, it considered that it also constitutes an interference with the right of exerting an economic activity for professional users and that this practice can be sanctioned by the unlawful competition law as it causes damage to the competitors.

Finally, the Italian privacy commissioner examined the case of a subscriber of a telephony company receiving, without his explicit consent, advertising messages on his mobile phone from the same telephony company. After having opposed unsuccessfully to such messages, the user has exposed the

18 § 30 of the Directive on data protection
19 § 35 of the Directive on privacy and electronic communications; On data: art. 2 lit. g, 6 e 9 Directive on privacy and electronic communications;
21 Judgement of the Landesgerich of Berlin, January 14 2003
22 For the distinction between private and professional users, see the Telefonwerbung judgment as well as the criteria developed there. Available on http://www.bundesgerichtshof.de/entscheidungen
23 http://www.garanteprivacy.it
case to the privacy commissioner. However, the commissioner was unable to produce a judgment as in the meantime the company ceased to send these messages.

The key elements emerging from these judgments are the following. The transmission of advertising messages through SMS can be considered 1) as an aggressive form of advertising and therefore fall into the application of unlawful competition law, 2) as an unjustified interference on the private life of the recipient and therefore be sanctioned by the privacy protection law and 3) they generate a problem of protection and use of the users private data.

Switzerland

The Swiss regulatory framework offers, at the time of writing, an incomplete protection of the privacy of mobile services users, in particular against mobile spam. The reason is that the current legislation has not foreseen the emergence of these new technologies and has not conceived rules applicable to the new cases brought by them. This raises the interesting issue of the new juridical problems brought by the emergence of new technologies and their treatment. Generally, there are two possibilities to deal with such juridical gaps: either these new cases are treated by interpreting the actual legislation and jurisprudence, or these cases are regulated by new legal disposition (Cottier 2001, p11; Uhlmann et al. 2003, p235).

In the case of mobile spam the actual laws are not always applicable by analogy of through a teleological interpretation to the mobile medium. For this reason the government has recently proposed a modification of the law in order to take into account this phenomenon. The proposed modifications will tackle the law on telecommunication (LTC), law on unlawful competition (LCSI) and the law on data protection (LPD)24. More specifically, this project intends to add the dispositions 45a and sqq. in the LTC concerning the protection of user data as well as the creation of a new disposition 3o of the LCSI which focuses on advertising messages sent without the consent of the recipient.

With the proposed modifications, Switzerland intends to align with the European legal framework by adopting the opt-in system. In particular, the sending of advertising messages is allowed if three essential conditions are respected: 1) the sender has the previous informed and specific consent of the user to accept such messages, 2) the sender is explicitly mentioned in the message and 3) in each message the user has the possibility to oppose (opt-out) to such messages easily and at no charge25. As in the European framework, there is the exception of the pre-existing commercial relationship which is applied using the same conditions as in the European legislation.

Concerning personal data, their protection is granted by three legal dispositions. The general principle is rooted in the application of the article on the protection of personality (art. 28 CC) and the law on data protection (art. 4 al. 5; 10a LPD). More specifically for massive electronic advertising (i.e. spam) the law on telecommunications (LTC) puts the burden of undertake appropriate measures to reduce this phenomenon on the shoulder of network operators. These can choose their measures freely, even tough the Federal Council has reserved the right to issue norms restricting their choices.

24 Message of the Swiss Federal Council of November 12 2003, appeared in Bundesblatt (i.e. the Official gazette of the Swiss Authorities) 2003 pp. 7253 sqq.
25 For a discussion of the different cases envisioned by this norm see also (Baudenbacher 2001, n7 sqq; Pedrazzini et al. 2002, p155 sqq.; Senn 2002, p90).
Concerning location data, network operators can use them to provide location-based services with the consent of the user. This consent, however, is not sufficient to allow the communication of these data to third parties and a specific consent must be agreed with each provider.

Finally, the Swiss legislation allows users to undertake a legal action against the senders on the basis of the violation of his data protection and personality protection rights. The sending of advertising messages through SMS is considered as one of such violations (Senn 2002, p91).

The United States of America

In the United States, the Congress considers that the email spam problem has reached overwhelming proportions. It is an effective and low cost communication medium for advertisers, while it generates huge annoyance and costs for the targeted users.

Conscious of this problem the industry issued a series of recommendations. For instance, the industry favored the publication of privacy policies and the establishment of privacy seals, such as trust-e, which should guarantee that the privacy policy is really adopted. Moreover, advertisers are advised to give users the possibility to object to receiving further messages through some form of opt-out. Actually, some senders give users the possibility to opt out, but there are senders who do not care about it. What is more, some even use the opt-out reply possibilities only to check that the email address is valid and use them for subsequent messages.

Given the ineffectiveness of industry self regulation practices, various States have issued their own regulation to reduce the spam phenomenon. However, this raises the problem of the heterogeneity of the legal framework adopted by the different states. In order to alleviate this problem, the Congress issued in 2003 the Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM Act) aiming at regulating the problem of spam nationwide. The CAN-SPAM Act now supersedes the more than 35 existing state spam laws. This act has become active since the first of January 2004.

In the CAN-SPAM Act the government makes the following considerations: 1) there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis; 2) senders of commercial electronic mail should not mislead recipients as to the source or content of such mail; 3) recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source.

This act envisions the opt-out system, allowing enterprises to send a first unsolicited message provided that they give the receivers the possibility to easily refuse to receive subsequent messages. This possibility is not limited as in the European legislation, but is extended to enterprises which do not have a pre-existing commercial relationship with the recipient. The spamming is thus allowed by legislation. Nevertheless the user has now an additional means to be protected from unwanted repeated violations its personal space, which may reduce the appeal for spammers to continue with their practices.

Furthermore, the Wireless Communication and Public Safety Act of 1999 specifies that the location information that a carrier has about a user when he makes a wireless call cannot be transmitted to third

26 Section 2 lit. B of the CAN-SPAM Act
27 Section 3.1 of the CAN-SPAM Act
parties without the user’s explicit authorization.

4. CONCLUSIONS

The right to privacy is universally recognized as being part of a more general right to the immunity of one's personality, which is a more fundamental and overriding principle than that of privacy.

This problem is also recognized by the various industry associations throughout the world. Guided by the dual goal of facilitating adoption of the proposed services by enhancing customers’ trust and avoiding more stringent regulation by the governments, they have issued guidelines to their members so as to provide a consistent protection of the user privacy.

However, recognizing the ineffectiveness of these industry self regulation practices, the various governments have issued laws specifically addressing the problem. These legislations are centered on the notion of user consent, even tough they differ for the modality and moment in which this consent must be collected. On the one hand, the European Union and Switzerland, have adopted fairly severe solutions based on the principle of the explicit opt-in which do not practically allow unsolicited messages except in restrictive conditions. On the other hand, the United States basically aligned on the industry regulation, by giving the opt-out recommendation a mandatory status and providing them an official legal power. This basically gives spammers the right to send one unsolicited message and require the recipient to request removal from the spammer's list. Unfortunately, recipients asking to be removed will be likely to get even more spam because the request will get them on a list of numbers known to be active which can be sold to other spammers, who can then send their first allowed messages. Table 1 summarizes the most salient differences between these regulatory frameworks.

<table>
<thead>
<tr>
<th>Principal laws</th>
<th>The United States</th>
<th>European Union</th>
<th>Switzerland</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Directive 2002/31/EC (Directive on electronic commerce)</td>
<td>LCSI (Law on unlawful competition)</td>
</tr>
<tr>
<td>Mobile advertising principles</td>
<td>Opt-out principle: unsolicited advertising on the mobile medium is allowed, provided that receivers are given the possibility to easily refuse to receive subsequent messages</td>
<td>Opt-in principle: advertising is considered unlawful except if the user has previously provided an informed and specific consent to receive such messages However, the legislation states the exception of the previously existing commercial relationship, where a first contact giving the possibility to opt-out is allowed.</td>
<td></td>
</tr>
<tr>
<td>Non commercial spam</td>
<td>The legislation essentially focuses on commercial messages. The application of spam measures to non commercial messages is open to question given the freedoms of expression, religion etc. contained in the First Amendment.</td>
<td>The law about unsolicited advertising focuses on commercial messages. However, non commercial messages can basically be treated in the same way in the view of a teleological interpretation of the norms.</td>
<td></td>
</tr>
<tr>
<td>Sanctions</td>
<td>The legislation contains both criminal penalties, to deter the most offensive forms of spam, as well as substantial civil penalties.</td>
<td>The legal sanctions of infringements to the above mentioned laws and the conditions for filing lawsuits against spammers are set by the single member states.</td>
<td>Legal sanctions to privacy infringements include both civil and penal sanctions.</td>
</tr>
</tbody>
</table>

Table 1: summary of the differences between legislations

Even tough the spam through SMS is not explicitly mentioned in any of the considered legislations,
which were primarily issued focusing on the use of email as the transmission medium, it can be considered in view of a teleological interpretation of the norms. The same problem lies with the treatment of non commercial unsolicited messages, which might be considered a spam even tough the norms explicitly address only commercial messages. To this point, the position of the United States legislation is open to question, given the freedom of expression contained in the First Amendment.

Furthermore, the discussion about recent judgments pointed out that the problem of spamming does not only infringe the rights of protection of privacy against unwanted intrusions and of personal data against unauthorized uses, but can also be tackled from the angle of unlawful competition.

It is clear that these new regulatory norms provide additional protection to the users. It is also evident that regulators must have intervened to try to reduce the emerging phenomenon of spam which has achieved preoccupying dimensions. However, it remains to be seen if this additional protection has a significant deterrent impact on spammers and if it contributes to enhance trust among users and thus facilitate their adoption decisions.

It is our personal conviction that the issuance of these new regulatory norms focusing on the spam problem are a necessary and important first step. We are also confident that the emergence of a body of judgments in favor of the protection of the privacy will have a profound impact on the various parties. Yet, the application of these rules must be done in a sensible manner. On the one hand, judges must avoid applying these norms with too much severity as there is a substantial risk of retarding or limiting the development of a very promising industry. On the other hand, with a loose interpretation of the norms, users’ may not feel enough protected to trust their service providers, which may also limit the development of the industry or confine it to a few well reputed players and limit the innovation often stemming from start-up enterprises.

Still, these new regulatory regimes might well not be sufficient if it they will not be accompanied by the creation of adequate technological or organizational means allowing an effective enforcement. As well, an information effort must be done to let all the involved parties – in particular the users, marketers and network operators – to become aware of their rights as well as their responsibilities.

As a concluding remark, we would like to remind that these regulatory frameworks have been developed as an ultimate barrier against privacy violations and that it is in the best interests of the industry to behave well so that there will practically be no privacy infringements. The reason is that once users feel to be exploited and lose trust in mobile service providers, it might be too difficult and expensive to recover them as valuable customers. In this view, it is encouraging to see that industry associations are well aware of the problem and try to put in place measures aiming at reducing the problem.

ACKNOWLEDGEMENT

The work presented in this paper was supported by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005-67322. As well, the authors would also like to thank the "Centre de Droit Privé" and Professor Bernard Dutoit of the University of Lausanne for the support and precious assistance in the legal aspects of mobile spam.
REFERENCES


Commission of the European Communities (2004). Communication from the commission to the European parliament, the Council, the European economica and social committee and the committee of regions on unsolicited commercial communications or ‘spam’. Brussels, Commission of the European Communities.


Verbiest T. (2003). *Publicité par courrier électronique: de nouvelles règles du jeu.* Available at: Last accessed on


Vogt C. (2002). *Privacy: An important but complex right.* Available at: http://archive.infoworld.com/articles/op/xml/02/03/08/020308opethics.xml, Last accessed on March 6 2004
