

Anti-spam laws at the times of social networks: the European approach

M.L. Lobina, D.D. Giusto
Department of Electric and
Electronic Engineering
University of Cagliari
Cagliari, Italy

D. Mula, E. Maggio
European Law School,
University of Rome, Italy
Rome, Italy

Abstract—Spam is the abuse of electronic messaging systems meant to their indiscriminate use. This practice is currently founding a fruitful demographic background when directed at the users of internet social networks as Facebook, MySpace and Twitter. Stopping spam is not easy although central governments are facing the problem with ad-hoc legal frameworks. This work presents what has been done in this sense by European central government also analysing in detail traits and statistics of the phenomenon.

I. INTRODUCTION

The term spam indicates something that keeps repeating and repeating to great annoyance and originally comes from the spam skit by Monty Python's Flying Circus on December 1970 [1]. The success of the sketch is probably the reason why 'spam' has been used to mean the first net abuse on May 1978 [2]. As reported by Templeton [1], this was the case of spam in the most accepted meaning of the term, that is an email sent to all the USA west coast ARPANET users. For many years the situation lasted unchanged with attempts of spam email and derived abuses, addressed to the closed communities of newsgroup users. Substantial changes are not detectable also in the very first years (i.e., 1994-1995) of the World Wide Web service.

A dramatic change in this scenario happened with the advent of social network sites around 1996 [3]. Such services focused on indirect ties by combining a network of personal profiles: an enormous quantity of possible spammable data was exposed for the first and at the same time to the risk of fraudulent spam activities. Starting from this moment it is possible to mention the term 'social network spam'. It is interesting to note as spam did not change its nature but only the manner in which it was spread. From a legal standpoint, as we shall see, this observation is fraught with meaning.

After twelve years the situation is much more complex with an increasing exposure of personal data in one of the global internet social networks. Furthermore, many useful instruments provided by such networks, as friendship invitation, internal messaging system or post walls, are by themselves a possible attempt to people privacy through spam. This results in a particular attention from many central governments, who respond by legislating to limit the diffusion of the phenomenon. Much of this term, despite created for different contexts,

can be effectively applied also to social network spam. This work studies the European legal framework, analysing both directives and ad-hoc reports from central agencies with the aim of providing a memorandum of what has been legally done.

The work is organized as follows. Section I provides a brief analysis of spread and use of social networks, together with some spam statistics and cost facts. Section II then analyses the ways spam can be perpetrated in a social network. Section III is the core of the study and presents the state of art of the European legal framework. Finally, last section draws our conclusions.

II. SOCIAL NETWORK AND SPAM FACTS

A spammer (i.e., a professional spam operator with a minimum of three terminated spam offenses to service providers) is always searching for new abuse possibilities. But, why choose a social network as target? This section tries an answer to the question.

Growth of member communities

Table I proposes a view of the main online sectors worldwide for biennium 2007-2008 by CNET [4]. Member communities have reached in 2008 over 5.4% points respect to 2007. The growth rate is more than twice that of any of the other four largest sectors. Apart from isolate statistics, at the moment of writing there is no an update of this complete view for 2009-2010, but the present situation suggests a similar trend also for this period.

Table I: Top 5 online sectors worldwide 2007-2008 (in %)

Sector	2007	2008
Search	84	85.9
General interest/Communities	83.4	85.2
Software manufacturers	72	73.4
Member communities	61.4	66.8
E-mail	62.5	65.1

Over this data, the relevant aspect is a change in the way people feel the social network. Firms are increasingly using social network software to share and collaborate. A Demos [5] research speaks of 'intuitive interaction', indicating the possibility of using built-in software to create closer links

and boost productivity. Regarding this aspect, a significant pointer is the average number of friends for user, as revealed by a recent research by HP Lab [6]. The same research shows Twitter users have an average of 80 friends, while a Facebook user does a little better with an average of 130 friends [7]. Both these statistics are not valid for long term period and must be updated at the time of reading this work. Social theory holds that groups of 100 to 150 are the most relationships that one individual can meaningfully hold. In fact, despite the numbers those that have over 100 friends most only communicate with a smaller subset of friends, and the rest is broadcasting to others (spam). Another interesting pointer is the number of new events created per unit of time. As an example Facebook has a an average of 100,000 new events per day [7], while the most prolific Twitter users post an average of 150 tweets/day [8].

Diffusion of member communities per country and age

Table II presents the diffusion of member communities for geographic area from a top-site estimation based on Alexa and Google Trend [9]. The second social network is strongly variable (as in Europe where it has leaved blank).

Table II: Social network diffusion per country (in %)

Country	Social Network 1	Social Network 2
EU	Facebook	-
USA	Facebook	MySpace
China	QQ	Xiaonei
Russia	V Kontakte	Oddnoklassniki
Australia	Facebook	MySpace
Canada	Facebook	MySpace

Table III presents the average access (average hours and pages for user) for geographic area [10].

Table III: Social networking audience per country (in %)

Country	Avg hours	Avg pages
Russia	6,6	1307
Canada	5,6	649
Finland	4,7	919
UK	4,6	487
USA	4,2	477
Australia	3,4	374

The Russian audience has the highest engagement among the 40 individual countries. Brazil, Puerto Rico and Spain are between Russia and Canada.

Considering the age, the social network audience is strongly changing depending on the considered network but a general trend is a shift from the young to the old. As an example, the greatest growth for Facebook has come from people aged 35-49 years of age (+24.1 million), while 50-64 year olds visitors present +13.6 million and under 18 year old visitors +7.3 million [11].

Categories and diffusion of spam

Although spam is a variable phenomenon (the reader is invited

to observe daily reports from sample honeypot domains [12]), a general trend can be depicted as in Table IV [13].

Table IV: Origin of spam (in %)

Country	Sept. 2009	Oct. 2009
USA	23	25
Brazil	12	12
India	4	4
South-Korea	5	4
Russia	-	2

These statistics refer to the whole spam phenomenon including social network spam. Comparing these data with Table III, it is evident there is no a direct link between the origin of spam and the audience of social network except marginally for USA (decreasing of 5% points from 2007 [14]).

Another observation is that overall percentage of spam, directly or indirectly linked to social networks, is much higher than imagined. This is the sneaky side of social network spam. A recent statistic, including also what produced by spambots, estimates as pure spam the following percentages of intra-social network messages: 15% percent in Twitter, 7% in Facebook and 10% in MySpace [15]. But once an user publishes his personal profile with an email contact, the spam arrives also from the outside the social network. The reader can found reliable statistics of email spam in [16], while a general classification is presented in [13].

Spam cost

Spam is an expensive phenomenon from the perspective of the victim and a fruitful business for spammers. The costs considered here include both the intra-social network and derivated (e.g., as email) spam abuses. The overall effort is a sum of three main contributions: user productivity (deleting spam, looking for false positives), help desk (IT helping end users deal with spam) and spam control software/hardware/service (plus licensing fees). In many cases there are no references to the wasting of bandwidth and money scammed to internet users. Also in this case, the data presented here are not valid for long term period.

Spam cost presents a general growing trend. The estimate from [17] shows a worldwide cost around \$100bn in 2009 with a 30% increase over 2007 and 100% over 2005 figures. A short-period analysis comes from the Q309 Postini report: levels remained steady during 2009 with little growth or decline depending on the short period [18]. These data are also confirmed by the European Network and Information Security Agency (ENISA) [19].

According to a study by the Radicati Research Group, a research firm based in Palo Alto (CA), spam costs businesses \$20.5bn annually only in decreased productivity as well as in technical expenses [20], while e-mail security market will grow from over \$4.4bn in 2009, to nearly \$6.7bn in 2013.

The conclusion is that a middle size enterprise has an average spam cost of \$182,500 per year and approximately \$41,000 per unit percentage of spam [21]. This is definitely an

enormous damage for a firm with a profit of \$30 per hour.

III. ANATOMY OF SOCIAL NETWORK SPAM

As said previously spam is a phenomenon that acts both inside and outside (e.g., derived abuses, as email spam) the social network. In this section we refer directly to the 'inside' aspect of spam.

Typology of social network spam

A social network has a structure made of individuals, which are connected by one or more specific types of interdependency.

Reached one node of the structure, it could be very easy to spread a message to the entire community. Common techniques used by spammers in social networks include [22]:

- 1) Use of spambots to automate friend invitations and comment posting.

- 2) The sending of notes typically including embedded links to pornographic or other product sites designed to sell something.

- 3) Friend invitations, using an attractive profile which is likely to persuade someone to accept the invitation.

- 4) Stealing members passwords to insert and promote their offers on another profile.

- 5) The posting of spam comments on public notes or comments areas of friends.

Spam in real social networks

As an example, we propose different forms of spam activity in Twitter, Facebook and MySpace.

Spammers can operate in Twitter in various ways. The basic approach is a short URL. In this case the limit of 140 characters on tweets is used to mask the real nature of the link. It is impossible to tell it contains a scam, virus, trojan, or other type of malware. Another approach is the hijacking of an account with large list of followers with the aim of sending out spam. Tweetjacking is similar to hijacking and occurs when spammers reply to a user's tweets with messages containing a short URL (see the first case). With 'hash tags on trend topics' spammers exploit the trending topic by adding a hash tag to a popular keyword in their tweet. This increases the visibility of spammers' tweets. The last approach is the 'follower fraud': the creation of an Twitter account is very easy and the spammers can be encouraged to automate the process and collect a massive amount of counterfeit followers (Friendbot has features to automate this). The aim is selling the account for a good amount of money and repeat the process to cultivate the spam group.

Facebook and MySpace present certain similarities with Twitter. It is possible to create an account and collect followers by automating the 'inviting friend' process [23] with a bot. The same category of applications can also be used to automatically login and post on lots of peoples walls the same message or send directly the same message.

Already, social network providers have implemented filters that attempt to slow the use of bots, and are aggressively

deleting spam accounts when discovered. Facebook has an internal 'Don't Go Overboard' mechanism for recognizing possible spammers and the hijacking of an account is definitely not simple.. However it could be realistic the problem of zombie botnet (as for MySpace).

Risks

The risks are broadly the same as with other kinds of spam: traffic overload, phishing and deviation to commercial URLs, loss of trust. This last aspect is particularly important as the presence of many fake profiles, diluting the social network, can delegitimize both the network structure and the 'normal' users. This is specifically the case of a reputation (i.e., Sybil) attack. Another risk is the evolution of social network spam in corporate espionage by means of social engineering methods (as a social network scam).

IV. THE EUROPEAN LEGAL FRAMEWORK

As many other countries worldwide also Europe protects personal data from unauthorized treatments. By definition any form of information, repeatedly sent without the permission of a subject, is considered unacceptable by both the subject and the provider of the service through which the information has been dispatched. Besides, even if available on a network, the profile of the subject is not usable without his prior permission for sending any information.

Currently, the standard reference is Directive 2002/58/EC [24] and is based on two cardinal principles, namely: a) sending any information must be authorized and empowered with the consent of the subject; b) there is no needing for the prior consent of the subject only when a person or organization, acquired legitimately the contact of the subject with an antecedent contractual relationship, use such data to market their services or similar products. There is always the possibility for the subject to object at any time to the data treatment. Consent may be given by any appropriate (Art.17) and user-friendly (Art.25) method enabling a freely given specific and informed indication of the subjects wishes. The rule of silence-consent is not permissible.

A person or organization can not in any way make the contract to the consent for sending information having a commercial nature. This statement refers to what is stipulated between the parties regarding information in Art. 10 and 11 of [25], stating the provider must indicate the mandatory or optional nature of providing data and the consequences of any refusal. Consent must be specific, thus the subject must be informed about the possibility his data are transferred to third parties, with particular attention to the scope of the treatment by such parties. Conversely, when the subject is not disclosed to this information, the third party can not use this information to send any form of information. This is specifically the case of users of social networks and spammers.

When a subject registers with a social network service and uses built-in instruments, it is revealed the risk that both the subject and the provider (i.e., owner and maintainer) can not have a full control over the treatment of the personal profile,

because a portion of profile is always visible to all the community. Thus, remaining in-force the previous legislative basis, a subsequent verification of [25] by European agency ENISA issued several guidelines on security and privacy aspects in social network services. This work produced in particular the study presented in [22]. Among many, the recommendations regarding the provider are mentioned here. First of all, a good provider should promote strong authentication and access-control. On all networks such methods can differentiate bona fide members from spammers. The so called 'white label' social networks (i.e., professional networks used as a basis for business contacts) are particularly involved in this. An overall stronger authentication process would also act as an incentive to enrolment in the network by increasing the trust placed in others on the community. The second aspect is guaranteeing the maximum possibility of reporting and detecting abuses of any form. Systems and policies for handling illegal action and bogus, breaking terms and conditions of the network, should be built into the design of the service. Reputation aggregation systems, or simply well-documented procedures, are examples of such systems. Finally providers should offer convenient means to delete data completely and set appropriate defaults. The last aspect is particularly important. In fact, few users change default settings therefore it is vital that these are made as safe as possible. These settings should also consider the age of the person signing up, since it may be appropriate to set different default privacy settings for minors. As an example a set of default settings and improvements to face application spam can be found in [23].

In 2008, the European Data Protection Supervisor considered it appropriate to intervene on the issue with a specific 'Resolution on the protection of privacy in social network services', adopted in October 2008, which contains a set of recommendations addressed to both users and operators of such services [26]. This work analyses in depth what happens from the outside of the social network and proposes a set of ten recommendations for social network providers. In fact, very little protection exists against abuses as copying any kind of personal data from other profiles and re-publishing the data elsewhere or crawling of users' profiles (one third of human resources managers already admit to verify and/or complete details of job applicants with data from social network services).

Furthermore, also after the deletion of the original profile from the network, copies may rest with third parties or with the social network service providers. In addition, some social network providers make user data available to third parties via application programming interfaces, which are then under control of these third parties.

An emphasis on creation and use of pseudonymous profiles, together with offering of encrypted connections for maintaining user profiles (including secured log-in), can be found in [27].

V. CONCLUSIONS

The success of social networks depends heavily on the number of users it attracts. The providers are encouraged to design behaviours which increase the number of users and their connections. This results in an over-exposure of personal profiles to various risks, including spam and social network spam. The situation is even worse because users are often not aware of the size and nature of the audience accessing their profile data. Furthermore, they feel an unjustified sense of intimacy created by being among digital friends. In a certain sense this could be considered a paradox, as the network of personal profiles is the most valuable asset for social networks but at the same time the primary reason of privacy and security abuses for network members. At first this work has analysed the traits of such abuse providing a quick analysis of related statistics, facts and techniques. Then the European legal framework has been detailed together with some recommendations from central agencies. What derives from all the legal and technical aspects cited in this paper is that the best prevention of social network spam is subject security awareness of the community to which he belongs. The social network providers should have a special responsibility to act in the interests of individuals using their networks by stimulating this sensibleness.

REFERENCES

- [1] <http://www.templetons.com/brad/spamterm.html>
- [2] <http://www.templetons.com/brad/spamreact.html>
- [3] Boid, D.M., Ellison, N.B., *Social Network Sites: Definition, History, and Scholarship*, Journal of Computer-Mediated Communication, VOL.11 2007
- [4] <http://ec.europa.eu/information society/policy/ecommtoday/framework/privacyprotection/spam/index-en.htm>
- [5] www.demos.co.uk/
- [6] Huberman B.A., Romero D.M. and Fang Wu, *Social Networks that matter: Twitter under microscope*, Journal on the Internet, VOL.14, January 2009
- [7] <http://www.facebook.com/press/info.php?statistics>
- [8] <http://sysomos.com/insidetwitter/mostactiveusers/>
- [9] <http://www.techcrunch.com/2009/06/07/a-map-of-social-network-dominance/>
- [10] comScore press, Russia has Worlds Most Engaged Social Networking Audience, July 2009
- [11] Nielsen, Global Faces and Networked Places - A Nielsen report on Social Networkings New Global Footprint, March 2009
- [12] <http://www.m86security.com/trace/spam-statistics.asp>
- [13] Symantec, A Monthly Report (34), State of Spam, October 2009
- [14] TrenMicro, Data Stealing Malware on the Rise Solutions to Keep Safe Businesses and Consumers, Focus Report Series, June 2009
- [15] <http://www.itwire.com/content/view/27782/1231/>
- [16] <http://www.spamcop.net>
- [17] <http://www.ferris.com>
- [18] <http://googleenterprise.blogspot.com>
- [19] ENISA, EU efforts called to avoid a 'digital 9/11', May 2008
- [20] <http://www.spamlaws.com/spam-stats.html>
- [21] <http://www.datamanager.it>
- [22] ENISA Position Paper No.1, Security Issues and Recommendations for Online Social Networks, October 2007
- [23] <http://blog.facebook.com/blog.php?post=10199482130>
- [24] Official Journal of the European Communities, Directive 2002-58-EC of the European Parliament and of the Council of 12 July 2002, July 2002
- [25] Official Journal L 281, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, November 1995

- [26] Data Protection and Freedom of Information Commissioner of the State of Berlin (Germany), Resolution on Privacy Protection in Social Network Services, 30th International Conference of Data Protection and Privacy Commissioners Strasbourg, 17 October 2008
- [27] International Working Group on Data Protection in Telecommunications, Report and Guidance on Privacy in Social Network Services - Rome Memorandum - 43rd meeting, 3-4 March 2008, Rome (Italy), 4 March 2008