The importance of Whois data bases for spam enforcement

Chris Fonteijn

Chairman OPTA

Joint meeting GAC/GNSO

Marrakech, Monday 26 June 2006

Introduction

My name is Chris Fonteijn and I am chairman of OPTA. I thank you kindly for the opportunity given to me to speak to you directly and discuss the subject of Whois databases with you on such a short notice. OPTA is the Independent Post and Telecommunications Authority, the National Regulatory Authority of the Netherlands. We are an independent agency, with no policy or legislative powers. Usually our name is associated with market analysis, tariffs and conflict resolutions between telecommunication companies.

In addition to these subjects OPTA has a legal task in consumer protection and most prominently in enforcing the anti spam articles in the Netherlands Telecommunication act. We were given this task in May 2004. We fight spam in its many guises, being all forms of unsolicited electronic communication in which a product is advertised in some form. Further we deal with spy ware, malware, say unwanted software, and direct marketing. We have powers under administrative law, not criminal law, meaning that we can levy fines and injunctions in case of infringement.

All our investigations in spam (related) matters start with research in Whois data bases. When we were informed of the preference in the GNSO to limit the Whois data to the technical contact details, the so-called narrow purpose definition, we became somewhat alarmed. It is our belief that if this definition is taken forward in the strict sense, spam enforcement, but also other forms of enforcement of internet and internet related abuse, will become more difficult nationally, but might well come to a

full stop internationally. In this presentation I will try to make clear how we use Whois data bases, what the consequences of a loss of access to these data are and finally give some suggestions for further discussion on the subject.

The Internet, of course, is one of the driving forces of modern society. It supports the global economy. But, it also threatens to become a virtual safe haven for criminals and abusers. We have been given a task in spam enforcement principally for reasons of consumer protection.

I would like to point out that it is not just my organization that became alarmed in our country over the past few weeks. I know that within the Dutch prosecutor's office and the police force the subject is considered as a grave set back. Within the European Commission and in the Working Party article 29 of the Data Protection Agencies in the EU the subject of law enforcement viz à viz privacy is under discussion also. I refer to the letter that was sent to you by the Working Party last week.

Spam enforcement in the Netherlands

- Identifiable Dutch spam has decreased by 85% over the past two years.
- So far we have received 15.339 consumer complaints.
- The Netherlands no longer appears in the world wide top 10 of spam sending countries. OPTA is actively investigating international spam facilitating companies and stopping this through injunctions imposed on these companies.

- OPTA plays an active role in international cooperation on spam in the Contact Network of Spam enforcing Authorities, the London Action Plan and advised on the OECD task force on spam. Also we have assisted in investigations of the FTC and the Australian spam enforcer and refer and accept cases.

OPTA and Whois

I cannot stress sufficiently the importance of the Whois databases for OPTA and comparable institutions. It is the starting point of all our investigations. My organization reacts to a complaint of a consumer on our complaint website. First we look to the Whois database to collect information on the website advertised in the spam. This means that a simple case, a case in which the spammer does not hide himself, is solved within minutes. A warning under threat of penalty is issued the same day. If the Whois data base were limited to technical data only, this would become weeks if not months, but also create considerable costs on all sides, as I will explain later.

The Whois is also used for more in depth information. Domain name registrations can be used to match registrations. For example it can be used to compile Whois history, by checking and comparing past and present registrations. This historical research has proven to be a successful tool. Spam has not always been forbidden by law. So along the way spammers have sometimes simply altered their registration and falsified their identity. But what is masked now, might have been openly available information in the past.

Spammers usually have many websites at their disposal. Mistakes are made, or patterns can be established because spammers for example use the same name, or registrations are from the same area each time when they fill out a form. In combination with further research this can lead to the true identity of the spammer. Even if all contact details are falsified it is often possible to establish a pattern in their many website registrations. Mind you, this form of research is only possible through Whois databases with the current level of information.

GNSO and Whois data

OPTA is worried about the definition as recently preferred in the GNSO. Why do we suggest opening it up for debate and look for solutions that accommodate these worries? I would like to point out the following.

- More complex administrative processes

Formal letters of inquiry need to be written by enforcers, requests have to be studied by the legal department of registrars. Possibly we need to enforce on basis of the Telecommunication Act in cases where information is being withheld by a registrar. A more complex administrative and judicial process on collecting and providing information is created. At present this is readily available.

- Loss of time and efficiency

This written process means a waste of time and efficiency, which slows operations down considerably. The search for historic data and establishing patterns becomes practically impossible. There will be no way of knowing what is out there any longer, because data cannot be linked easily.

- Increased burden and costs on registrars

The registrar at this stage plays a minor role, because most of the information we need is publicly available. The burden and the ensuing cost of the more complex process are all on the registrar who has to accommodate information requests.

- Increase in international information requests

Since spam is a cross border phenomenon we will probable have to obtain most of our information from abroad after the Whois data is limited. In countries with a spam law it is likely that we can ask our colleague enforcer to assist in obtaining information, but it has to fit into their workload. The burden and cost are put on them instead and after that on their local registrar. In this way more time is lost in assembling the most elementary information on a spammer.

- OPTA can not enforce abroad

Cross border OPTA does not have the powers to enforce and not all our international colleagues have the same powers we have. This means OPTA can not obtain information on a registered spammer if someone abroad decides not to cooperate.

The enforcement action is likely to come to a full stop and the spammer continues his business in safety.

The conclusion is that in general it will become harder to assemble information and cross border it will become very difficult to impossible.

Discussion

Privacy is an important issue. We, of course, have an obligation to work according to the EU legal framework as implemented in Dutch national law. Privacy sensitive information can only be used within the context in which we obtained it or was handed over to us. OPTA has signed a Protocol on Cooperation with the Dutch Data Protection Agency in 2004 especially because of spam (related) investigations and the sensitivity of personal data that is involved. The protocol of cooperation between CNSA members also deals with the cross border aspects of privacy. But we would like to point out that enforcement of spam, spy ware and malware, as well as enforcement of breaches of law under the criminal code like phishing, d-dos attacks and botnets, also improves privacy protection. We would ask you to also focus on that aspect. We respect privacy. Only in the event of complaints made we would use the Whois information to track down the spammer. Ultimately isn't spam sending also a breach of the privacy of the recipient by the spammer? Therefore, should the spammer have a right to privacy protection from the enforcement point of view? We do respect his privacy in case of a fine, by not publishing all private personal data. OPTA is are also aware of the many other interests, but a common interest is the

reduction of spam around the world. Having said this, is there a solution foreseeable that is as well proportionate as accommodating to law enforcers?

Tiered access, in which the full Whois databases can be accessed by accredited and selected law enforcement agencies and others with similar interests, could possibly be a solution to this problem. To me this seems like a proportionate solution. The letter recently sent to ICANN by Peter Schaar, chairman of the article 29 Working Party of EU Data Protection Agencies, suggests that such a solution is in line with the opinion of the Working Party.

Another important subject that could be discussed is the accuracy of data in the Whois data bases. In what way can the quality of registrations be bettered and or more strictly imposed on the registrars and registrants? There are registrars in the world who are notorious for not cooperating with spam enforcers. It is no coincidence that many spammers register their websites with these registrars. Is this a subject that could be discussed with ICANN?

Finally, please allow me to point to ICANNs By Laws. In Section 2 under Core Values it says, among others, “ICANN works on the preserving and enhancing of the reliability and the safety of the Internet”. This happens to be the line of business we are in: making the Internet more reliable and safe for consumers. I would suggest and offer to you to start looking together for ways to ensure this for the future. We are willing, for example through the CNSA, to work together with ICANN and the GNSO

in finding ways to ensure that the internet can remain reliable and safe whilst respecting privacy. This by no means seems a paradox to me.

I would like to conclude in stressing once again how important the current Whois data bases are for our work in spam enforcement. Fighting spam helps making the Internet safer for consumers. A safer Internet means economic growth as well as an enhanced privacy protection. OPTA feels it needs to be able to do his work and you can contribute to make sure we can. So let us, together, look for and find ways to achieve an optimal solution, which does justice to all needs.

I thank you for your attention.

Chris Fonteijn

Chairman OPTA