Policy on Internet security: obligation for Dutch ISPs to provide information about spam, botnets and zombies

Gerrit-Jan Zwenne (gerrit-jan.zwenne@twobirds.com) is a Partner at Bird & Bird LLP and associate professor of telecoms and privacy law at Leiden University.

Out of growing concern for Internet security, the Dutch Telecoms Regulator, OPTA, issued new guidelines on January 14, 2009. The authority published a new set of guidelines on Internet security which are applicable to Internet service providers (ISPs), including the providers of mobile Internet.

Previous attempts

This is not the first time OPTA has tried to address the issue of Internet security. Its first attempt to set rules and guidelines for Internet security resulted in a lot of criticism and discussion, particularly regarding OPTA's powers in this area and its approach to the issue.

As a result, OPTA withdrew its initial proposals and the State Secretary of Economic Affairs, Mr. Heemskerk, invited interested parties from within the industry to put together their own self-regulating policies. However, although many of the ISPs did extensively discuss and debate the issue amongst themselves, they ultimately did not reach agreement and no self-regulation was established.

Policy guidelines

A little over one year later, OPTA has again taken up the issue and published its policy guidelines regarding ISPs' obligations to provide information about Internet security. In brief, OPTA wants ISPs to improve the information provided to consumers about Internet security. According to OPTA, the average Internet end user does not have sufficient know-how or information on how he or she can protect themselves against Internet security risks, such as:

- spam
- botnets
- phishing
- spyware
- trojans
- router security
- identity theft, and
- unsolicited websites.

In addition, OPTA clarifies what action it will take if, providers in its opinion, do not fully comply with their obligation to provide relevant Internet security information. Sanctions include imposing an order for periodic penalty payments to force a provider to improve the information provision.

Survey

Before issuing its policy, OPTA conducted a survey of approximately 35 ISPs' websites to determine to what extent they complied with the minimum information requirements. The majority of the ISPs did not comply with the obligation to provide Internet security information and information that was provided, proved insufficient. In particular, OPTA concluded that the providers of mobile Internet did not provide adequate information.

In March 2009, OPTA will look at whether the situation has improved. In view of positive reactions, OPTA expects that ISPs will cooperate and make improvements to the Internet security information they provide to their clients.

Of course, Internet security issues are obviously not just a problem generated from the lack of information available for consumers. Even if end-users are informed about the risks of spam and botnets, they will still suffer from it. Clearly, to really improve Internet security, more action must be taken. It is therefore expected that OPTA will draft further measures asking providers to trace and remove botnets.

Processing employee biometric data in Poland

By Krystyna Szczepanowska, Partner, and Lukasz Czynienik, IP/TMT department Lovells, Warsaw.

Introduction

For the last two years, we have observed in Poland the growing interest in the use of biometric readers; as a convenient way of monitoring the working hours of employees or for limiting access to firms' rooms and databases. Such devices are used not only in the private sector, but also in schools, universities, hospitals and state administrative offices.[1]

There are opposing views to consider. On the one hand there are employees' fears supported by the position of the Polish Personal Data Protection Authority ("GIODO") and the Polish Ombudsman ("RPO") for appropriateness in processing biometric data for these purposes. On the other hand, there are rational arguments from employers for whom devices using employees' biometric data are a relatively cheap, reliable and