Dutch telecoms regulator wants to enforce Internet safety requirements - ISPs not enthusiastic

Zwenne, G.J.; Erents, C.

to the assignment of claims does not apply to the assignment of contracts. In fact German contract law provides that the assignment of a contract requires customers' consent. Frequently customer contracts contain wording sufficient for contract law standards but often fail to meet the quality requirements of consent under data protection rules. At present an argument can be made that the performance of a contract which contains an assignability clause requires that the transfer of the customer data is possible to complete all rights and obligations resulting from such contract, in order to overcome the data protection hurdle.

A corresponding argument can be drawn from Article 7(b) of the European Data Protection Directive (Directive 95/46/EC) as implemented into the FDPA. Following the reasoning of the above court decision, a second argument seems possible. Just like German contract law takes precedence over the FDPA to allow the assignment of claims, it may also prevail over the FDPA in case of the assignment of a contract, if such assignment is made in compliance with German contract law. The German Civil Code provides in Section 309 No. 10 German Civil Code (BGB) that assignment clauses contained in consumer contracts are valid if they either name the third party to which the contract may be assigned or if they give the consumer the right to withdraw from the contract on the occasion of the assignment. Arguably also Section 309 No. 10 German Civil Code prevails over the rules of the FDPA. In other words, should Section 309 No. 10 German Civil Code be respected, there is no room for additional legal hindrances based on the FDPA.

At least from a consumer customer's perspective there is no apparent reason why the transfer of the consumers data as a consequence of the assignment of a claim should be less intrusive to the consumers privacy than the transfer of basically the same data as a consequence of the assignment of a contract to which such claim might relate. On this basis an argument can be made that a distinction between a customer contract with a consumer (which could be assigned) and a customer contract with a company (which could not be assigned) would equally be unreasonable. Thus, the court may decide in the future that under certain conditions (*i.e.* the assignment stays within the statutory limits constituted by Section 309 German Civil Code) the assignment of a customer contract in consumption of an asset deal is not subject to the FDPA just like the assignment of a payment claim of the same contract in a securitisation transaction is now no longer (and should never have been) subject to the FDPA.

THE NETHERLANDS

Dutch telecoms regulator wants to enforce Internet safety requirements – ISPs not enthusiastic

Gerrit-Jan Zwenne (gerrit-jan.zwenne@twobirds.com) and Chris Erents (chris.erents@twobirds.com) from Bird & Bird Solicitors provide an update on how the Dutch regulator is getting tough on protecting consumer safety on the Internet.

Internet safety is high on the agenda of the Dutch telecoms regulator, OPTA. After fighting spam with some success and an occasional failure, the Dutch telecoms regulator now wants to enforce Internet safety requirements. The Dutch Telecoms Act requires that all telecoms providers take appropriate technical and organisational measures to ensure the safety and protection of their networks and services. In doing so they have to guarantee a level of security and protection which is proportionate to the risks involved, taking account of the state of the technology and the costs.

Apparently, the regulator feels that currently, the ISPs have not taken enough effective steps to protect their subscribers and end-users. Therefore the regulator proposes a policy consisting of a minimum set of compulsory measures. This new policy, which is now the subject of a public consultation process, was preceded by a survey carried out by an independent research bureau, Stratix. This survey showed that the main threats consist of 'malware' and 'crimeware', *i.e.* software that is sneakily and clandestinely installed on the end-users' PCs via viruses and contaminated websites. Infected PCs (zombies) are then used by cybercriminals for the distribution of spam, distributed denial of service attacks (DDoS-attacks), or phishing, collecting identity details like usernames, passwords, creditcard numbers etc.

To prevent the installation of such malware and crimeware OPTA wants the ISPs to comply *inter alia* with the following requirements:

- no forwarding of traffic from IP addresses that do not belong to their own IP series to other networks (so-called 'egress filter'),
- no forwarding of incoming traffic from IP blocks that are not assigned or are not in use (so-called 'ingress filter'),
- providing virus and spam filters for all incoming email,
- providing information (on a regular basis) to new and existing subscribers about concrete threats and the possible protective measures against these threats.

In a hearing about this proposed policy, the Dutch Consumers' Association, Consumentenbond, showed some enthusiasm about the policy proposed by OPTA and the consumers' representative expressed its appreciation of this first step by OPTA. However, the association does expect that more far-reaching measures will be needed to deal effectively with current threats.

A different view was presented by the XS4ALL, an ISP well known for its commitment to digital rights and the free and uncensored exchange of information. The ISP's representative first pointed out that on the basis of current telecoms regulations, OPTA may not have the authority to issue the intended policy, let alone to enforce it. Moreover, XS4ALL criticised OPTA's approach to the threats, as this was exclusively directed at ISPs and not also to other stakeholders, such as subscribers and end-users, hard and software providers, e-banking services, the government and the like. In addition to this, the ISP argued that most measures proposed by the telecoms regulator are already implemented by the ISPs. This shows that the ISPs particularly are very well capable of implementing necessary measures without formal regulation. Therefore the ISP characterised OPTA's initiative as unnecessary, redundant, superfluous, or in short: 'overregulation'.

Perhaps as a result of the ISPs's limited enthusiasm, the responsible State Secretary recently announced his intention to amend the Telecoms Act and other telecoms regulations, and include more detailed rules regarding Internet safety. The State Secretary has the intention to provide OPTA with the legal instruments to enforce minimum security standards. Additionally, the State Secretary announced that he will establish a central coordinating point, called the National Infrastructure for Cybercrime. The aim of this infrastructure is to enable an efficient and effective exchange of information on Internet security and threats.

Obviously, such initiatives may very well help to make the Internet safer and more secure. However, when it comes to security the 'human factor' should not be ruled out. This was perfectly shown by OPTA itself, when it informed more then a hundred interested parties about the results of the hearing and the consultation process. It sent out an email message with all the email addresses of the recipients in the 'to:' field instead of the 'bcc:' field. And, by doing so, the red-faced regulator unintentionally exposed all recipients' email addresses, which were subsequently used by XS4ALL to bring its views on the matter to their attention.[2]

1 OPTA's consultation document regarding Internet security (in Dutch) can be downloaded from *www.opta.nl/asp/besluiten/consultatiedocumenten/-document.asp?id=2375*

2 The views of XS4ALL can be found at *www.xs4all.nl/opinie/2007/05/18/opta-zoekt-werkgelegenheid-deel-2*

