INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Are we fighting spam with the right weapons?

Australia, the UK and the US all have legislation to fight spam, but is there evidence that the threat of fines actually makes a difference? **Laura Linkomies** investigates.

The United States has witnessed yet another spammer go down. In January, a man based in Florida was fined $11.2 billion for sending millions of unsolicited e-mails that advertised mortgage and debt consolidation services. The fine is likely to be the biggest ever imposed for sending spam. In Europe, the Netherlands has been heavy handed with spammers; in 2004 a fine of €42,500 was given to an individual for spam that praised Hitler's book *Mein Kampf*. Both countries have legislation in place to fight spam, and are vigorously enforcing the regulations. On the other hand, the UK, which also has resorted to legislating against spam, lacks sufficient enforcement powers and is not seeing similar results. Is it even possible to tackle spam due to its international nature and the problem of identifying the offenders?

Under the US federal Controlling the Assault of Non-Solicited Pornography Act (CAN spam), it is not illegal to send unsolicited commercial e-mails, but action can be taken against spammers who provide false contact details or forge a company's domain name. In addition to the federal-level regulation, most US states have their own laws on spam.

The Federal Trade Commission (FTC) has been active in suing spammers for unfair or deceptive trade practices ever since the Act entered into force in 2004. Its recent report to Congress, "Effectiveness and Enforcement of the CAN-spam Act", claims that the Act is effective in providing protection for consumers, and that the Act is being enforced aggressively by state and federal law enforcers and the private sector. (See www.ftc.gov/reports/canspam05)

Alisa Bergman, Partner at law firm DLAPiper in Washington DC, told *PL&B* that she agrees with the findings in the FTC report.

"Our experience indicates that the notice and opt-out requirements overwhelmingly are being followed by legitimate marketers, with most marketers honouring the requests within the 10-business day time frame.

"In addition, successful enforcement technology has played a leading role in combating spam. For example, e-mail authentication technologies hold a great deal of promise for addressing some of the issues raised by spam."

So far, the FTC has brought 21 cases under the CAN-spam Act. The first prosecutions under the Act in 2004 gave a promise of real enforcement effort, as the FTC cracked down on two of the then largest spammers in the world, Phoenix Avatar and Global Web Promotions, whose operations had generated nearly one million complaints to the FTC. Since then, several substantial fines have been imposed. But does it actually stop spam?

"Most of the prosecutions in the US have been about peripheral matters under CANSPAM Act, rather

Continued on p.3

Issue 81 **February/March 2006**

NEWS & ANALYSIS

LEGISLATION & REGULATION

MANAGEMENT & STRATEGY

CONSULTATION & INITIATIVES

TECHNOLOGY

Austria's Supreme Court stops a Private Investigator exploiting mobile-network data

By **Rainer Knyrim**, Partner, and **Christian Podoschek**, Associate, at Preslmayr Attorneys-at-Law, Vienna. Preslmayr advised and represented T-Mobile Austria GmbH in the proceedings.

As already briefly reported in the December issue of the International Newsletter (p.6), the Austrian Supreme Court recently stopped a private investigator who was using T-Mobile Austria's internal network data (case 4 Ob 113/05d, September 15 2005). The case addresses burning legal questions arising from internal data included in many computerised systems such as telecommunication networks. While the case was argued on unfair competition grounds, there was the possibility of also arguing the case on data protection grounds, including T-Mobile's rights as a legal person.

To understand clearly the issues in this case, it is first necessary to explain the technical basics.

In every mobile phone network, transmitting stations are identified by a unique code, called a "Cell-ID". Besides the Cell-ID the mobile phone also receives a country code and the operator's individual number, ensuring that the phone uses only transmitting stations in the correct network. Every mobile phone in range receives and internally processes the Cell-ID. The Cell-ID is usually invisible for users of phones, but can be revealed by using a code or special software on the phone. These codes or software tools, although intended only for use by authorised personnel, are sometimes available through certain non-official internet resources.

A private investigator had a clever idea to exploit T-Mobile's network to his benefit. He modified his mobile phone to display the Cell-ID and hooked it up with a laptop computer and a GPS-navigation system. Driving around Austria with his equipment, he logged most Cell-IDs in T-Mobile's network and linked them with the geographic coordinates received through the GPS-system, finally collecting this information in a database. His intention was to offer all kinds of "Location Based Services", ranging from surveillance of persons and vehicles to logistic applications. Buying or renting his system enabled his customers to track the position of a mobile phone which was modified accordingly, using a convenient web-interface. It was also possible to combine tracking positions into a tracking route.

T-Mobile Austria did not accept this system and sued the private investigator for injunctive relief, based upon Art 1 of the Austrian Statute on Unfair Competition. Besides the defendant arguing that there was no competition between him and T-Mobile, the discussion focused on whether T-Mobile's Mobile Network Data, especially the "Cell-ID", was free to use for regular customers or not.

> "Based on Art.27 of the Austrian Statute on Data Protection, T-Mobile could have demanded that the private investigator delete all the data he collected, thus eliminating the basis of his system of Location Based Services."

The defendant was a T-Mobile customer. He paid a monthly basic charge plus call-charges for every phone call and SMS. However, T-Mobile's standard contracts allow the customer to use the mobile phone network only for the specified services, which are basically phone calls and SMS, and maybe E-Mail and internet services with more advanced types of mobile phones. Using the network for any other purpose is not permitted. For Location Based Services that are offered by T-Mobile, customers have to pay an additional fee. But in the defendant's opinion, he did not have to pay more because he thought that the "Cell-ID" was free for everybody to use. He argued that the Cell-ID as a concept of the GSM standard had not been invented by T-Mobile and there were no copyrights that apply, describing the Cell-ID as a "waste product".

Mobile phone networks cannot be bought "off the rack". Building a mobile phone network requires, besides the respective licenses, intensive individual planning and development work. A network plan needs to be drafted, and suitable locations for transmitting stations must be evaluated. Finally, after building the transmitting stations and interconnections, software programs have to be set up and configured with the appropriate data. Creating the "network-architecture" incurs great expense and demands countless hours of engineers' work. In addition to that, the costs of the ongoing operation of a mobile phone network must be considered. T-Mobile and other mobile phone network operators build and operate the network-architecture to offer a wide range of telecommunication services, including the so called "Location Based Services" which the private investigator wanted to sell to his customers as well.

The Austrian Supreme Court finally agreed with T-Mobile and stated that the private investigator's system violates the Austrian Statute on Unfair Competition and prohibited the further operation and marketing of the system.

By getting access to the Cell-ID in T-Mobile's network, simply copying and using this Cell-ID data to operate his own system for Location Based Services, the private investigator unlawfully exploited T-Mobile's network architecture. The Supreme Court especially focused on the link between the Cell-ID and the geographical position of the transmitting station. This link is the key to many services which T-Mobile and other mobile phone operators offer to their customers. The Cell-ID data had not been received by the defendant accidentally. He fully intended to "crack" the code that usually hides the Cell-ID from normal mobile phone users. Consequently, data which determines the network architecture of a mobile phone network is not a waste product but rather an essential element of the operator's product.

The case was compared with a Supreme Court ruling of 1998 (4 Ob 237/98a). In that case, company A was offering a cashless payment system for shops, using ATM-cards which were handed out to customers. The customer's bank name and account number were stored on the magnetic strip on the back of the card. Company B, which was later successfully sued for injunctive relief by company A, developed equipment to read the bank name and account number from the ATM-cards, offering a cheaper cashless payment systems to store owners. The Supreme Court ruled that B exploited A's work, violating Art 1 of the Austrian Statute on Unfair Competition, similar to the private investigator's case. For the cashless payment system, the magnetic strip and the data held on this strip was the key to the services offered, just like the link between Cell-ID and geographic position is the key to the Location Based Services in a mobile phone network.

Austria's data protection laws would have provided for an alternative way to shut down the private investigator's system. The collected Cell-ID data, especially the link between the Cell-ID and the geographic position, is individual-related data (Art 1 sec 1 of the Austrian Statute on Data Protection, 2000), because the data can be clearly assigned by T-Mobile. A Cell-ID is somehow like a transmitting station's zip code. The Austrian Statute on Data Protection not only protects human individuals, but also legal entities. T-Mobile and other mobile phone network operators obviously have a strong and understandable interest in keeping the Cell-ID data confidential. In our opinion, this confidentiality is worthwhile to be protected in the sense of the Austrian Statute on Data Protection. Based on Art.27 of the Austrian Statute on Data Protection, T-Mobile could have demanded that the private investigator finally delete all data he collected, thus eliminating the basis of his system of Location Based Services. However, as the unfair competition lawsuit was successful, a further claim based on data protection rules was not filed by T-Mobile.

We believe this decision's guidelines may be applied to many other similar cases. Today, countless commercial products are based upon computerised systems. Companies invest large sums into developing such systems. If copying a part or all of the system's logic or data enables competitors to provide similar services at less cost and effort, laws against unfair competition and also data protection laws provide a good defence.

Indian data protection amendments set for current legislative session

India's legislature is set to debate amendments to the Information Technology Act 2000 which would be the country's first law to specifically address data protection principles, explains Tejas Karia, Advocate and Solicitor at one of India's leading law firms. **Stewart Dresner** reports

Karia, speaking in London on February 9, explained how privacy issues were currently covered indirectly by a wide range of other laws. Some date back to the Penal Code of 1860, covering Breach of Trust and the Contract Act of 1872, which includes the remedy of damages for breach of contract. Others are much more recent, such as the Information Technology (IT) Act 2000.

Karia explained that the National Association of Software and Service Companies (NASSCOM) argues that India's outsourcing business could accelerate even faster if foreign companies had greater certainty regarding privacy laws. A problem now is that it is difficult to enforce contractual provisions regarding protection of personal data.

In a case involving stolen credit card data, a call centre employee, Asif Azim was convicted by a Delhi Court in March, 2003, one of the first conviction for cyber crime in India. He used a US citizen's credit card to make online purchase from Sony. He was traced through the call centre's IP address and was convicted on the basis of the 1860 Penal Code's provision on "cheating".

Business leaders argue that India would be able to attract even more call centre and Business Process Outsourcing work if the country adopted a privacy law which would help create more confidence among investors and foreign companies. The great prize is an adequate level of data protection to satisfy the European Union. As such a standard is far away, there is discussion in India as to whether it could enter into a Safe Harbor arrangement with the EU on the US model. However, Karia said that no such negotiations had begun.

Should enforcement in India be based on statutory rights or contractual rights; the US Safe Harbor principles or the data quality principles in the EU Data Protection Directive? This uncertainty is the reason for the Expert