crowell moring

CLIENT ALERT

Privacy & Data Protection

Dec.01.2009

Other sections of this issue:
Privacy & Data Protection | ISP-Liability & Media Law | Electronic Communications & IT

Protest against Belgian transposition of Directive 2006/24/EC on the retention of data

Directive 2006/24 requires the operators of publicly accessible electronic communication networks to retain traffic and location data for various services in order to serve the investigation, detection and prosecution of serious crime. This Directive is being transposed into Belgian law, but evokes protest by several organizations.

Background
On 15 March 2006 the European Union formally adopted Directive 2006/24/EC, on "*the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*".

This Directive seeks to harmonize the provisions of the Member States concerning obligations incumbent on the providers of publicly available electronic communications services or public communications networks with respect to data retention. More specifically, it requires these operators to store certain data which is generated or processed in their networks to serve the investigation, detection and prosecution of serious crime.

The Directive affects traffic and location data in various areas: fixed network telephony, mobile telephony, as well as Internet access, Internet e-mail, and Internet telephony (e.g. Skype) for a time period between six months and two years. According to article 5 of the Directive the following categories of data should be retained:

- Data necessary to trace and identify the source of a communication (e.g. the calling phone number, the user ID);
- Data necessary to trace and identify the destination of a communication (e.g. the number dialed, the name and address of the subscriber or registered user and user ID of the intended recipient of the communication);
- Data necessary to identify the date, time and duration of a communication (e.g. date and time of the log-in and log-off of the Internet access service together with the IP address and the user ID);

- Data necessary to identify the type of communication (i.e. the telephone or Internet service used);
- Data necessary to identify the communication device (e.g. the calling and called telephone numbers);
- Data necessary to identify the location of mobile communication equipment (the location label).

Article 2 of the Directive stresses that it shall not apply to the content of electronic communications, including information using an electronic communications network.

The Member States of the European Union had to transpose this Directive into national law by 15 September 2007, but could postpone the application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 15 March 2009.

Protest against the Belgian transposition
The Belgian legislator has failed to transpose this Directive into national law in a timely manner. A preliminary draft of law and royal decree have been heavily protested by several human rights organizations, the Association of Physicians, the Association of the Flemish Bars and the Association of Flemish Journalists together with their French speaking opponents:

(a) Infringement of the right on privacy

According to these organizations, the overall obligation to retain data constitutes a severe infringement of the right on privacy foreseen in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and article 22 of the Belgian Constitution. Even though the Directive explicitly states that no data revealing to the content of the communication may be revealed, it is, according to these organizations, possible to get a clear view on certain aspects of a person's life by consistently taking note of traffic or location data.

Moreover, from a technical perspective the border between content and traffic or location data is sometimes blurred in modern electronic communication infrastructures and the Directive is deliberately vague on the technical aspects underlying the gathering of these data.

The organizations state that the overall retention of these data does not comply with the principles of necessity and proportionality, since it is not proven that the same result would not be reached by using less restrictive means, such as data preservation (i.e. the retention of data in case of concrete indications of certain felonies and after the authorization of an independent judge).

(b) infringement of the professional secrecy

In the opinion of the relevant organizations, this obligation interferes with the professional secrecy of physicians, lawyers, journalists and clergymen, as well as all political and business activities that demand secrecy. This would be particularly true for the Belgian transposition since this draft, contrary to the Directive that emphasizes that these data can only be used in case of "serious crimes", allows for the use of these data for practically all crimes.

(c) high costs

The overall retention of data will have enormous financial implications for Telecom operators and Internet providers. Unless they receive a contribution from the government, these operators will pass this extra cost on to the consumer. Thus, in the end it will be the tax payer or the consumer that pays for it.

(d) The overall retention of data is not effective in the battle against crime

According to these organizations, the period of retention of the relevant data is so long that it will almost be impossible to find the right information in these enormous databases. It will also be very hard, if not impossible, to link the obtained information to the final user. Moreover, traffic and location data can be forged or manipulated easily. People with a certain basic knowledge would even be able to stay unnoticed on the basis of the data obtained within the framework of the overall retention obligation foreseen in the draft of law.

In sum, the draft of law is, according to the relevant organizations, technically thoughtless and will prove to be impracticable. Therefore, they have started several actions in order to urge the Belgian government not to transpose this Directive into national legislation and to take the initiative at the European level to modify the relevant Directive.

Links:

- http://www.bewaarjeprivacy.be

For more information, contact: Anke De Boeck.

Online statements: website operators beware!

The English Court of Appeal, in a recent judgment in Gary and Karen Patchett v. SPATA [2009] EWCA Civ 717, confirmed that website operators may, in certain circumstances owe users a duty of care, breach of which may be actionable.

Introduction

Swimming Pool & Allied Trades Association Ltd ("SPATA") runs a website www.spata.co.uk providing details of companies who are involved in the installation, design and construction of swimming pools.

The claimants (a husband and wife) found SPATA's website through a Google search and short-listed three contractors whose details were listed on SPAT's website and which were stated to be members of SPATA.

The applicants eventually contracted with Crown Pools Limited ("Crown"), who they thought was a member company of SPATA, to construct the swimming pool in the garden of their home. The family paid Crown part of the agreed fee for the work but before the pool was finished, Crown stopped its operations because it was in financial difficulties. As a result, the applicants had to retain other contractors to complete the work, paying additional amounts. A claim against Crown, an insolvent company, would be futile so the applicants brought a case against SPATA.

SPATA's website contained a number of representations including statements that "SPATA approves member companies who specialise in undertaking pool contracts for commercial use" and "[o]nly SPATA registered pool and spa installers belong to SPATASHIELD, SPATA's unique Bond and Warranty Scheme offering customers peace of mind that their installation will be completed fully to SPATA Standards - come what may!". Mr Patchett claimed that these statements induced him into selecting the three contractors, and eventually, Crown. Subsequently, it turned out that Crown was not an approved member of SPATA, that SPATA had not vetted Crown and that Crown was not covered by the SPATASHIELD. The applicants claimed that misrepresentations on SPATA's website amounted to negligence on behalf of SPATA.

Importantly, SPATA's website also contained a statement, referred to as 'paragraph 8', that "SPATA supplies an information pack and members lists which give details of suitably qualified and approved installers in the customer's area" and that the pack includes the list of questions the customers should ask contractors before and after retaining them. If the information pack would have been requested, the applicants would have discovered that Crown had not been vetted by SPATA. The applicants, however, did not apply to SPATA for the information pack.

Findings of the Court

The novelty of the case was that the Court applied the traditional law of negligence principle of the duty of care to website operators. The Court examined "whether there was a sufficient proximity between [SPATA and the applicants] and whether it would be fair, just and reasonable to impose a duty of care upon SPATA" and concluded that there was no duty of care but only because of the 'further enquiries' statement on the website.

The applicants argued that it was "reasonably foreseeable to SPATA that such people would rely upon the representations in order to decide what action to take." Lord Clarke, however, held that "while SPATA no doubt knew that the representations on the website would be likely to be acted upon by people like the claimants, it would not expect them to do so without further enquiry."

The Court found that the 'paragraph 8' statement urged customers to conduct a further independent enquiry even though there was no specific wording to this effect. Interestingly, Lady Justice Smith, dissenting, found that SPATA had breached its duty because the statement about 'further enquiries' merely offered the information without making it compulsory or necessary for the customers to obtain the information pack.

Significance

The Court confirmed that information on the website should be read 'as a whole' and not in a piece-meal fashion. Secondly, it is quite possible that in the absence of a paragraph inviting further enquiries by customers, SPATA would be found as owing the duty of care and liable in negligence in this case.

Website operators should not only ensure that their website statements are accurate and not misleading, but also where they are broking or introducing the services of others, ensure that customers are urged to make further enquiries to the relevant service provider directly. To this end, the website should display a clear and prominent message and disclaimer which leaves no doubt that further enquiries by the customers are necessary.

France: 10.000 Euro fine for illegally installing a CCTV system in clothes stores

Throughout Europe, privacy legislation imposes various obligations with respect to the installation and operation of CCTV systems at both publicly accessible premises (e.g. in stores) as well as non-publicly accessible premises (e.g. offices). Violations of these obligations may lead to warnings and/or financial sanctions and, moreover, result in bad publicity, for instance when the decisions imposing sanctions are made public.

Facts

A complaint had been filed against a clothing manufacturer with three stores in the Paris area, employing 30 people. The complaint was based on the absence of declaration with the French data protection authorities ("CNIL") of a CCTV system, as well as on several other violations of the law because of the way the system was used.

The plaintiff alleged that the cameras installed by the company continuously filmed the premises, both publicly accessible and non-accessible parts thereof, including places reserved for the personnel where no goods were stored.

The CNIL consequently performed an investigation, including a search at the premises. The CNIL found that the system was composed of 23 cameras, installed in 1980 and 2007 at the registered seat of the company and in three stores. The images were indeed continuously registered.

The investigations of the CNIL confirmed that certain cameras indeed filmed locations open to the public (entrance of the stores, the shop itself), and that others focused on places where only personnel was allowed, also where no goods were stored (hallway, storage room, ateliers for the creation of goods). It was established that the president and managing director of the company could log in on the system from a distance and view the images via internet. The images were also accessible from two supervision posts. At the entrance, the computer for this supervision was accessible without password. Two servers were also freely accessible. The investigation showed that images were continuously stored for seven days after they were filmed.

The system was indeed not declared with the CNIL and the authorization required for the installation of the system under French law was not available.

Further, the investigation confirmed that the notification of the processing to the persons filmed, as required by law, was insufficient because hidden behind the counter of the store, so that it was almost not visible. No notification could be found at the entrance. Moreover, the information provided to the employees was insufficient or even non-existing. The communication in the employment agreements of persons hired after the installation of the CCTV system was too general and the personnel hired before the installation, where the employment agreement did not hold such general clause, were not informed at all.

The CNIL therefore sent a warning to the company, asking to, within a month:

- proceed with the prior declaration with the CNIL for all processing performed, and, in particular, the CCTV system;
- take all necessary measures so that the CCTV system's purpose would be limited to the combat of theft, and would not result in the employees being constantly monitored;
- remove all cameras the presence of which is not justified by the above purpose;
- inform the CNIL of all measures taken by the company to inform the persons filmed;

- take all measures required to ensure the security and confidentiality of the personal data collected, so that only the persons that need to know, given their function, would have access;
- justify with the CNIL that all the above has been respected.

The company did react and did undertake certain actions to cope with the comments of the CNIL, but these have been found to be insufficient by the CNIL. Consequently, the CNIL has fined the company for the reasons set out below.

Decision of the CNIL

In particular, the CNIL decided:

- Personal data should be collected and processed in a loyal and lawful way. The data have to be collected for well-determined, explicit and legitimate purposes and cannot afterwards be treated for purposes that are incompatible with these purposes.

  Although the company was asked (i) to take all measures so as to ensure that the system would only be used for the combat against theft and could not result in the employees being constantly monitored, and (ii) to remove the cameras that would not serve this purpose, the company did not take any measure to limit the monitoring of its employees.

  The company alleged that the use of the cameras concerned would also be justified by the 'manipulation of goods' and the 'free movement of public and personnel'. According to the company, only the offices of the administrative personnel would not be the subject of camera monitoring.

  However, the CNIL found that it resulted from the declarations of the company that the offices were nevertheless permanently filmed, so that the personnel was constantly monitored by the employer. Such processing, according to the CNIL, is excessive, so that the system is not strictly limited to the combat against theft. The CNIL therefore decided that French privacy law was violated on this point.
- The company has the obligation to inform the data subjects of the processing, including e.g. of its purpose.

  The CNIL had to conclude that the information given to the employees by the company, even after the CNIL's notice, was still manifestly insufficient. The purposes of the processing, the persons for whom the images were intended and the actual modalities of the access right of the data subject, were not part of the information.

  The CNIL therefore again decided that French privacy law was violated.
- With respect to the security and confidentiality of the processing, the CNIL found that after its notice to the company, the company did indeed isolate its servers and did limit the access to the images to certain representatives of the company, using passwords. Consequently, the CNIL decided that on this point, the company conformed with the notice.

  For the above violations, the CNIL decided to impose a 10.000 Euro penalty. It was also decided that the CNIL's decision had to be published on the CNIL's website and on the website of Legifrance.

* * *

Throughout Europe, privacy legislation imposes similar obligations with respect to the installation and operation of CCTV systems at both publicly accessible premises (e.g. stores) as well as non-publicly accessible premises (e.g. offices). Violations of these obligations may lead to warnings and/or financial sanctions and, moreover, result in bad publicity, for instance when the decisions imposing sanctions are made public.

For more information, contact: Frederik Van Remoortel.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Thomas De Meese
Partner – Brussels
Phone: +32.2.282.1842
Email: tdemeese@crowell.com