BNA International

# World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 5, Number 4 April 2005

## Articles

### Legislation & Guidance



### Personal Data



### Security & Surveillance



## Case Report

### Legislation & Guidance



## News

### Legislation & Guidance



### Security & Surveillance



www.bnai.com

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A.

*Publishing Director:* Deborah Hicks
*Editorial Director:* Joel Kolko

*Editor:* Nichola Dawson
*Production Manager:* Nitesh Vaghadia

**Submissions by Authors:** The editors of *World Data Protection Report* invite readers to submit for publication articles that address issues arising out of the regulation of data protection, either on a national or transnational level. Articles with an appeal to an international audience are most welcomed. Prospective authors should contact Nichola Dawson, World Data Protection Report, c/o BNA International Inc, 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, England. Tel. (+44) (0)20 7559 4807; fax (+44) (0)20 7559 4880; or e-mail: nicholad@bna.com. If submitting an article by mail please include a diskette with the article typed in plain text or in Microsoft Word or WordPerfect formats.

**World Data Protection Report** is published monthly by BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A. Administrative headquarters: 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, England. Tel. (+44) (0)20 7559 4801; Fax (+44) (0)20 7559 4840; e-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116.

Subscription price: U.K. and rest of world £625; Eurozone €995; U.S. and Canada U.S.$1,045. Additional copies of this publication are available to existing subscribers at half price when they are sent in the same envelope as a standard subscription.



Website: *www.bnai.com*
*ISSN 1473-3579*

**The U.K.** Government has come under considerable pressure of late to ease the prohibition on the evidential use of intercept material. The Parliamentary Committee on Human Rights, the Director of Public Prosecutions, Human Rights organisation, Liberty, and the Metropolitan Police Commissioner are just some of those who oppose the prohibition.

With this in mind, we are pleased to include a timely review of the U.K. Regulatory Investigation of Powers Act (RIPA) by Richard Budworth, beginning on page 3.

The transfer of personal data is the topic of our article by Christoph Rittweger and Michael Schmidl, also in the Legislation & Guidance section this month. The article offers a detailed analysis of the impact under German law of the E.U. Standard Contractual Clauses on the use of data processors outside the EEA.

The retention (or not) of communications data by telecoms operators has been a contentious issue in the European Union since the 1997 Telecommunications Privacy Directive provided that E.U. Member States had the possibility, but not the obligation, to retain such data for law enforcement purposes.

A divide has sprung up between the law enforcement authorities and intelligence agencies on the one hand, who advocate the retention of *all* communications data, and service providers and privacy advocates on the other, who oppose the financial costs and privacy violations that such a degree of control might herald. The issue has also raised concerns for employers in Europe - namely if they too could be subject to the same type of obligations when providing Internet access to staff. Our article by Karin Retzer and Cyril Ritter discusses the recent Paris Court of Appeal judgment in *BNP Paribas v. World Press Online*, which focuses on this exact question.

Finally, our thanks go to Thomas Smedinghoff for his excellent commentary on the Expansion of Corporate Information Security Obligations and to Alessandro del Ninno for an update on the latest regulations governing the processing of personal data in Italy.

Nichola J. Dawson

**We wish to thank the following for their contribution to this issue:**
*Richard Best,* Ashurst, Frankfurt; *Richard Budworth,* 11, Old Square, Lincoln's Inn, London; *Christopher Kuner,* Hunton & Williams, Brussels; *Julia Meuser,* Freshfields Bruckhaus Deringer, Hamburg; *Elizabeth McNaughton, Andrea Freund, Ian Hay* and *Veera Rastogi,* Blake, Cassels & Graydon LLP, Toronto; *Alessandro del Ninno,* Studio Legale Tonucci, Rome; *Karin Retzer* and *Cyril Ritter,* Morrison & Foerster, Brussels; *Christoph Rittweger* and *Michael Schmidl,* Baker & McKenzie, Munich; *Kerstin A. Zscherpe* and *Andreas Splittgerber,* Baker & McKenzie LLP, Frankfurt/Munich.

# Legislation & Guidance

## The U.K. Regulation of Investigatory Powers Act 2000

*By Richard Budworth, a barrister at 11, Old Square, Lincoln's Inn, London. The author may be contacted by e-mail at budworth5@aol.com*

Not until the Interception of Communications Act 1985 ("the 1985 Act") was there any legislative control of the interception of communications. The Human Rights Act 1998 and the need for compliance with the European Convention on Human Rights ("ECHR") was the main catalyst behind The Regulation of Investigatory Powers Act 2000 ("RIPA").[1] The reverse suffered by the United Kingdom in the European Court of Human Rights related to an unwarranted interception by the police of a senior police officer's office telephone.[2] The interception of a private telephone, unregulated by statute, was not "in accordance with the law" and was thus an interference with the officer's right under Article 8(1). Section 1(3) of RIPA deals with this deficiency, and gives the subject of the interception a civil remedy.

RIPA covered the whole field of interception, as well as other forms of surveillance. Unlike the 1985 Act, RIPA defined interception in section 2(2).

RIPA also made express provision for private as well as public service providers.[3]

All the essential features of the regime established by the 1985 Act for the issue of warrants by a secretary of state were preserved by RIPA.[4] Section 65 established a Tribunal with greatly enlarged jurisdiction, as compared with 1985 Act.

It can be thus seen that RIPA has emerged from an incremental response over the years by Parliament to adverse ECHR rulings.

The purpose of this paper is to review RIPA, which has been described by the House of Lords as perplexing and difficult to construe with confidence.[5]

### When and How Interception Takes Place

#### Section 1

Interceptions of postal services, public and private telecommunications systems are criminal offences under sections 1(1) and 1(2); while section 1(3) creates a civil liability.

Section 1(5) of the Act permits interception without a warrant if:

> "(a) it is authorised by or under section 3 or 4;
>
> (b) it takes place in accordance with a warrant under section 5 ("an interception warrant"); or
>
> (c) it is in exercise, in relation to any stored communication, of any statutory power that is exercised (apart from this section) for the purpose of obtaining information or of taking possession of any document or other property".

The obtaining for example, of a production order under Schedule 1 to the Police and Criminal Evidence Act 1984 for stored data to be produced.[6]

The latter would cover circumstances where, for example, a person has been arrested in possession of a pager and the police believe that the messages sent previously to that pager may be of assistance in the case. In these circumstances, the police would be able to apply to a circuit judge for an order under Schedule 1 to the Police and Criminal Evidence Act 1984 for the stored data to be produced.[7]

A person would have "lawful authority" for the interception of a communication within section 1(5)(c) where the interception was carried out in performance of his obligation under paragraph 11 of Schedule 9 to the Police and Criminal Evidence Act 1984, not to destroy material to which an application for an order under paragraph 4 of that Schedule related; if a telecommunications company served with notice of an application under Schedule 9 was only able to avoid destruction of the e-mails to which the application related by "intercepting", then it had lawful authority to do so.[8]

Section 1(6) allows a person with a right to control a private telecommunications network to intercept on their own network without committing an offence.

#### Section 3

Under section 3(i) certain kinds of interception are authorised without the need for a warrant:

- where both parties, sender and intended recipient, have consented, or there are reasonable grounds for believing that both parties, have consented;
- either party has consented, and the interception has been authorised under Part II of RIPA;

(Such a situation might arise where the police wish to intercept the call of a kidnapper, who is telephoning the relatives of a hostage. This would be authorised as surveillance rather than by an interception warrant.[9])

- authorises interception where it takes place for the purposes of providing or operating a postal or telecommunications service.

The Post Office may need, for example, to open a letter to discover the address of the sender because the recipient's address is unknown.[10]

For lawful interception which takes place without a warrant, pursuant to sections 3 or 4 or pursuant to some other statutory power, there is no prohibition on the evidential use of any material that is obtained as a result. The material may however be excluded under section 78 of the Police and Criminal Evidence Act 1984 ("PACE") or pursuant to the Human Rights Act 1998.[11]

### Section 4

Under section 4(1) an interception of a communication in the course of its transmission by means of a telecommunications system is authorised if:

> "(a) the interception is carried out for the purpose of obtaining information about the communications of a person who is, or who the interceptor has reasonable grounds for believing, abroad;
>
> (b) the interception relates to the use of a telecommunications service provided to persons in that country or territory which is either-
>
> - (i) a public telecommunications service; or
> - (ii) a telecommunications service that would be a public telecommunications service if the persons to whom it is offered or provided were members of the public in a part of the United Kingdom;
>
> (c) the person who provides that service (whether the interceptor or another person) is required by the law of that country or territory to carry out, secure or facilitate the interception in question".

This subsection will allow the United Kingdom to comply with Article 17 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

Section 4(2) enables the Secretary of State to make regulations setting out those circumstances where it is lawful to intercept communications for the purpose of carrying on a business. These regulations apply equally to public authorities. Their purpose is to make an exception to the basic principle, enshrined in RIPA, that communications may not be intercepted without consent.[12]

### Lawful Business Practice Regulations 2000

The Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations 2000 (SI 2000/2699) authorise, under regulation 3(1), businesses (which include public authorities, charities, and other non-commercial bodies) to monitor or record all communications transmitted over their systems without consent for the following purposes:

- establishing the existence of facts;
- ascertaining compliance with regulatory or self-regulatory practices or procedures;
- ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system;
- preventing or detecting crime;
- investigating or detecting unauthorised use of the business's telecoms system;
- ensuring the effective operation of the system;
- monitoring communications for the purpose of determining whether they are communications relevant to the system controller's business;
- monitoring communications made to a confidential counselling or support service which is free of charge.

The business must, under regulation 3(2)(c), make all reasonable efforts to inform every person who may use the telecommunication system that interception may take place.

### Section 5

Section 5 (1) states that,

> "subject to the following provisions of this Chapter, the Secretary of State may issue a warrant authorising or requiring the person to whom it is addressed, by any such conduct as may be described in the warrant, to secure any one or more of the following-
>
> (a) the interception in the course of transmission by means of a postal service or telecommunications system of the communications described in the warrant;
>
> (b) the making, in accordance with an international mutual assistance agreement, of a request for the provision of such assistance in connection with, or in the form of, an interception of communications as may be so described;
>
> (c) the provision, in accordance with an international mutual assistance agreement, to the competent authorities of a country or territory outside the United Kingdom of an such assistance in connection with, or in the form of, an interception of communications as may be so described;
>
> (d) the disclosure, in such manner as may be so described, of intercepted material obtained by any interception authorised or required by the warrant, and of related communications data.
>
> (2) The Secretary of State shall not issue an interception warrant unless he believes-
>
> (a) that the warrant is necessary on grounds falling within subsection (3); and
>
> (b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.
>
> (3) Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary-
>
> (a) in the interests of national security;"

("National security" is the term used in Article 8 of the Convention.)

> "(b) for the purpose of preventing or detecting serious crime;"

(This again reflects the provision in Article 8 "for the prevention of disorder and crime" but is qualified by the word "serious".)

> "(c) for the purpose of safeguarding the economic well-being of the United Kingdom".

It is not enough under subsection (3) that the warrant might be useful in supplementing other material, or that the information turned up could be interesting. "Necessary" reflects the wording of Article 8 of the Convention – "necessary in a democratic society" while proportionality, under Convention case-law, is an essential part of any justification of conduct which interferes with an Article 8 right.[13]

Under sub-section (5) a warrant shall not be considered necessary on the ground falling within subsection (3)(c) only if the information which it is thought necessary to obtain relates to the acts or intentions of persons outside the British Islands.

It would not therefore cover domestic events. Again the wording of section 5(3)(c) reflects the wording of Article 8.[14]

> "(4) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any warrant shall include whether the information thought necessary to obtain under the warrant could reasonably be obtained by other means."

### In the Course of Transmission

Section 2(1) defines a telecommunication system in the following terms:

> "Any system … which exists … for the purpose of facilitating the transmission of communications by any means, involving the use of electrical or electromagnetic energy."

Section 2(2) states that:

> "a person intercepts a communication in the course of its transmission by means of a telecommunications system if, and only if, he-
>
> (a) so modifies or interferes with the system, or its operation,
>
> (b) so monitors transmissions made by means of the system, or
>
> (c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,
>
> as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication".

Section 2(4) states that the interception takes place in the United Kingdom if the interception is effected by conduct in the United Kingdom and the communication is either:

> "intercepted in the course of its transmission by means of a public postal service or public telecommunications system; or
>
> intercepted in the course of its transmission by means of private telecommunications system in a case in which the sender or intended recipient of the communication is in the United Kingdom".

Section 2(6) states that the attachment of any apparatus to any part of the system is a modification.

Section 2(7) expands the phrase "while being transmitted", which is used in subsection (2). The times when a communication is taken to be in the course of its transmission include any time when it is stored on the system for the intended recipient to collect or access. This means that an interception takes place, for example, where an electronic mail message stored on a web-based service provider is accessed so that its contents are made available to someone other than the sender or intended recipient, or where a pager message waiting to be collected is accessed in that way. However, if a stored communication is accessed in this way, that conduct may be lawful by virtue of section 1(5)(c).[15]

Section 2(8) states that for the purposes of this section the cases in which any contents of a communication are to be taken to be made available to a person while being transmitted shall include any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently.

In the Committee stage of the Bill, "in the course of transmission" was defined as ending once sound waves were emitted by the telephone speaker. It was explained in this way:

> "The phrase 'in the course of its transmission' by means of a postal service or telecommunications system has been carefully chosen by Parliamentary counsel to cover a particular set of circumstances. The course of transmission begins where a postal service or telecommunication system first begins to transmit a communication. In a telephone, the sound waves from the human voice first begin to be in the course of their transmission by means of a telephone conversation when they are received by the microphone in the hand set. They continue to be in the course of their transmission until they are emitted by the speaker. Such phraseology ensures one is not technically intercepting a communication if one is in the same room as someone using a telephone and one happens to overhear what is being said. In the same way, listening to a voice from speakerphone is not interception: the sound waves have left the communication system on which they were transmitted and hence no longer technically in the course of transmission. That is what we have in mind, and why we have used the phraseology".[16]

A police officer, having attached a recording device to the telephone, intercepts that conversation but, possibly, not in the course of transmission. In MacDonald, the recording or interception was deemed to have taken place 29 milliseconds after it had left the telecommunications system.[17] It has been argued that this technical interpretation illustrates perfectly the weakness of RIPA which while embracing the language of ECHR rights, fails to provide the substantive protection required by the Convention.[18] RIPA makes crude physical distinctions between, for example, placing a device on the system and in the earpiece; between surveillance in a residential dwelling and on other private premises.[19] These distinctions fail to take account of the substance of the ECHR privacy protection which is based on the suspect's ability to foresee with a reasonable degree of certainty the consequences of his actions.

Section 2(2) would appear to protect the 'communication', namely two people talking on a telephone rather than any individual electrical pulse or signal. In MacDonald, this protection appears to be ignored in favour of drawing a technical line between the voice and the recording thus ruling out any "interception".

The tape recording of a telephone call by one party to it, without the knowledge of the other party, does not amount to interception of a communication within this section. This is surveillance not interception.[20]

In Hammond, Mclintosh and Gray, where a telephone call was recorded, the court also interpreted "interception" narrowly in holding that no interception had occurred as no third party was involved and the officer had consented to the recording.[21] Section 3, however, does not deny that an "interception" has taken place, rather it legitimises that interception with a party's consent. There is nothing in the Home Office notes on RIPA to suggest that a third party is necessary in these circumstances. Furthermore, this interpretation appears to ignore section 2(8) which expressly refers to the diversion or recording of the

contents of communications, in the course of transmission, to third parties. An interpretation which sets so much store by the words "while being transmitted" must take account of section 2(8).

In *R v. E*, a listening device was placed in the accused's car, which provided recordings of words spoken over two periods, one of about four weeks and the second about four days.[22] The Crown wished to adduce those recordings in evidence. The accused was recorded talking into his mobile telephone as well as to others in the car, whose words were also recorded.

It was submitted that the accused's mobile telephone calls were "intercepted" in which case they were either authorised by a warrant of the Secretary of State, under section 5 of RIPA, or, if not, the police officers were committing an offence of unlawful interception. In either event, the evidence of the intercepted calls was inadmissible under section 17. The critical issue was whether there was interception.

The court held that the natural meaning of "interception" denoted some interference or abstraction of the signal, whether it was passing along wires or by wireless telegraphy, during the process of transmission. The recording of a person's voice, independently of the fact that at the time he was using a telephone, did not become interception simply because what he said goes not only into the recorder, but, by separate process, was transmitted by a telecommunications system. This view was consistent with the words "in the course of transmission", found in the offence-creating section, section 1(1), and "while being transmitted", found in sections 2(2) and 2(8). Furthermore, under section 2(2), interception was concerned with what happened in the course of transmission by "a telecommunications system".

What was recorded in this case was what happened independently of the operation of the telecommunications system. The recordings were not made in the course of transmission. What was being recorded was not the transmission but the words of the accused taken from the sound waves in the car.

This case was identical to *R v. Smart & Beard* where a listening device was placed in a suspect's car which recorded speech between the occupants of the car and when one or other of them was using a mobile telephone.[23] It was held that there was no interception of an electrical impulse or signal passing through a telecommunication system. The voices from the sound waves in the car were recorded but the transmission was not. This surveillance evidence could therefore be used in court. Many would say that this rather artificial and narrow distinction between interception and surveillance illustrates the absurdity of RIPA.

Very recently in *R v. Allsopp* and others, the Court of Appeal have re-iterated that the plain words of RIPA require some interference in the telecommunications system. In this case a conversation had been overheard by police officers by means of an intrusive surveillance device.[24]

Has the Court defined "interception" too narrowly? Should as a matter of principle recording a call from the earpiece be treated as equivalent to the recording from within the system; should it constitute an interception?

Given the definition of "in the course of transmission" in the Committee stage of the Bill, it is difficult for courts to interpret the recording of a call from the earpiece as an interception. The definition is circumscribed and only, it is submitted, allows for a narrow interpretation. That said, section 2(8) sits uneasily with this definition and interpretation.

In enacting RIPA, as already seen, the Government embraced ECHR rights, in particular Article 8, in broad terms[25] and implemented Article 5 of the European Union's. Telecommunications Data Protection Directive, which requires Member States to safeguard the confidentiality of communications. This generous embrace of the right to privacy was, it is submitted, bound to clash with the narrow definition of interception in the Committee stage of the Bill.

## Admissibility of Evidence

The exclusion of interception evidence is contrary, many would argue, to the basic principles of evidence, namely, if it is relevant it is admissible. It is routinely used in the United States, where it has helped secure convictions in New York Mafia trials. Intercept evidence has also proved a valuable source of evidence in France and Australia. The counter-argument is that the use of intercept evidence would reveal the authorities' capabilities, prompting criminals to take more effective evasive action.[26]

Section 15 has the effect of restricting the use of intercepted material to the minimum necessary for the authorised purposes.[27]

Section 15(3): The general rule is that intercepted material must be destroyed as soon as its retention is no longer necessary for a purpose authorised under the Act.

The explanatory notes to the Act make it clear that all copies of any intercepted material must be destroyed.[28]

Section 15(4) states that,

> "something is necessary for the authorised purposes if, and only if-
>
> (a) it continues to be, or is likely to become, necessary as mentioned in section 5(3)".

This applies:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime;
- for the purpose of safeguarding the economic well-being of the United Kingdom;
- of giving effect to the provisions of any international mutual assistance agreement.

Section 15(4)(d) states that something is necessary to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution.

The general rule is that neither the possibility of interception nor intercepted material itself play any part in legal proceedings. This is set out in section 17, which excludes evidence, questioning, assertion or disclosure in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under RIPA. This means that neither the prosecution nor the defence can use the intercepted material. It preserves "equality of arms" under Article 6 of the ECHR.[29]

Section 17 (1) essentially repeats in expanded form (the italicised words) the contents of section 9 of the Interception of Communications Act:

> "17(1) Subject to section 18, no evidence shall be adduced, question asked, assertion or *disclosure* made or *other thing done* in, for the purposes of or in *connection with any legal proceedings* which (in any manner)-
>
> (a) discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or
>
> (b) tends (apart from any disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur".

Section 18 contains exceptions to this rule. The most important is subsection 7(a) which provides that intercepted material obtained by means of a warrant and which continues to be available, may, for a strictly limited purpose, be disclosed to a person conducting a criminal prosecution. Section 18(7) refers to-

> "(a) a disclosure to a person conducting a criminal prosecution for the purpose only of enabling that person to determine what is required of him by his duty to secure the fairness of the prosecution".

The exception is limited to securing the fairness of the prosecution. The material cannot therefore be used to mount a cross-examination, or retained in the possibility that it might be relevant for future proceedings. The general rule, under section 15, is that the material will be destroyed, and the exceptions, as already noted, only come into play if the material has been retained for an authorised purpose. The relevant authorised purpose here is for preventing or detecting serious crime (s.5(3)(b)) not gathering material for the purpose of a prosecution. The material may have already been destroyed in keeping with section 15(3). Under section 18(7), the prosecutor can only consider material that "continues to be available". This is intercepted material retained for an authorised purpose. The prosecutor, once informed, will decide whether the material affects the fairness of the proceedings.

The prosecutor may need to refer the material to the trial judge. Section 18(7)(b) recognises that a judge may need to be given access to the intercepted material where there are exceptional circumstances making that disclosure essential in the interests of justice. The judge having seen the intercepted material may require the prosecution to make an admission of fact. The admission will be abstracted from the interception; but, in accordance with the requirements of section 17(1), it must not reveal the fact of interception (s.18(10)). Nothing in these provisions allows intercepted material, or the fact of interception, to be disclosed to the defence.

In *R. v. W*, Attorney-General's Reference (No 5 of 2002),[30] the court considered the extent to which section 17 prohibited questions at trial concerning whether the telecommunication system involved was public or private. W distinguished Preston and allowed an inquiry at the trial into the public/private nature of the interception. This was upheld recently in *R v. E*, in which the House of Lords ruled, inter alia, that this issue was essential to the conduct of a fair trial and would not imperil the secrecy of the system by which warrants were issued to permit interceptions. Where there had been an interception on a private telecommunication system, it was possible in criminal proceedings to ask questions or adduce evidence to establish that it had been carried out by, or on behalf of, the person with the right to control the operation or use of that system.[31]

Section 17 (2) states that,

> "the following fall within this subsection-
>
> (a) conduct by a person falling within subsection (3) that was or would be an offence under section 1(1) or (2) of this Act or under section 1 of the 1985 Act;
>
> (b) a breach by the Secretary of State of his duty under section 1(4) of this Act;
>
> (c) the issue of an interception warrant or of a warrant under the 1985 Act;
>
> (d) the making of an application by any person for an interception warrant, or for a warrant under that Act;
>
> (e) the imposition of any requirement on any person to provide assistance with giving effect to an interception warrant".

Subsection (3) "The persons referred to in subsection (2)(a) are-

> (a) any person to whom a warrant under this Chapter may be addressed;
>
> (b) any person holding office under the Crown;
>
> (c) any member of the National Criminal Intelligence Service;
>
> (d) any member of the National Crime Squad;
>
> (e) any person employed by or for the purposes of a police force;
>
> (f) any person providing a postal service or employed for the purposes of any business of providing such a service; and
>
> (g) any person providing a public telecommunications service or employed for the purposes of any business of providing such a service".

Section 17(2)(a) only prohibits revelation if the interception is or would be an offence. A controller, therefore, properly authorised, who, intercepts private communications would not be committing an offence, and there would be no bar on disclosure. This may be a simplistic conclusion as the court may argue that there were unresolved issues to do with consent, the controller, and whether there was an interception, which would be forbidden by section 17.

It has been argued that there is a degree of incoherence between section 17, which shrouds interception offences in secrecy and section 18(4), which specifically excludes from that secrecy disclosure of intercepts when authorised under ss.1(5) (c), 3 and 4.[32]

There is no doubt that the recent ruling by the House of Lords is an authoritative statement that the purpose behind section 17 is to protect the secrecy of the warrant. The policy behind the legislation is of paramount importance in any interpretation of this statute. Obtaining a warrant for an interception guarantees that the product of the intercept remains inadmissible. Intercepting a private communication without a warrant, on the other hand, is a tort which would result in the admissibility of the evidence. Conceivably a senior police

officer could be encouraged to commit a tort in order to obtain the evidential fruit of the intercept.

It has been argued that there is something inherently illogical in a scheme which seeks to authorise an activity (ss.1-9), recognises that such an activity must lead to material which will be relevant at trial (s.18), and yet seeks to suppress that material and even the fact of its existence (s.17).[33]

Sections 17 and 18 seek to limit the use of material gathered from telephone intercepts to an "intelligence" rather than an "evidential" role. RIPA is thus viewed as a statute designed to optimise crime control.[34] It is difficult to see how this can optimise crime control in terms of securing convictions, when the product of interception cannot be used as evidence.

The narrowness of the definition of "interception" necessarily allows interception by many other methods; this has the effect of artificially restricting the admissibility of intercept evidence. At the moment, telephone conversations on an internal network, tape-recorded conversations in a person's house that are transmitted elsewhere and evidence from devices not attached to telephones are all admissible. In short, as long as the transmission is not recorded, the evidence is admissible. This resulting muddle has given RIPA a bad name.

## Human Rights

The driving force behind RIPA was the need to comply with European Convention on Human Rights ("ECHR"), in particular Article 8, the legal right to respect for a private and family life.

RIPA, as already seen, specifically implemented Article 5 of the Telecommunications Data Protection Directive ("the Directive"), which requires Member States to safeguard the confidentiality of communications.[35] Article 5, sub-para (1) reads:

> "Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance or communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14(1)".

Interference with Article 8 rights will be justified where it is in accordance with law and necessary for the purposes, inter alia, of the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others. It has been frequently held that to be in accordance with the law, regulations governing interception of communications must be particularly precise.[36] Interceptions not so regulated will breach Article 8.[37]

Article 8, like the Directive, also protects the call or the communication irrespective of the contents, and the identity of the caller. Substance of the privacy protection is based on the suspect's ability to foresee with a reasonable degree of certainty the consequences of his actions.

What privacy rights do suspects have in relation to their telephone calls being relayed to third parties? There is authority which impliedly reasons that a suspect should be taken to accept the risk that the contents of his call might be relayed to third parties.[38] It has been argued that there is a qualitative difference between merely listening and providing an account from recollection and a permanent recording of a suspect's conversation, and that the suspect should not be held to have impliedly consented to the latter.[39] Is the suspect's privacy protection under Article 8 destroyed by his acceptance of the risk? To say that it was would be a narrow interpretation of Article 8 and would sit uneasily with the court's decisions on that Article.[40] Again, Article 8 protects the call irrespective of the contents and the identity of the caller.

It is difficult to achieve compatibility with Article 8 when there is held to be no interception owing to technical interpretations under RIPA.[41] There is nothing to suggest that the means by which a telephone conversation is transmitted affects the protection afforded by Article 8.[42] In *A v. France* a telephone conversation was intercepted using a tape recorder. It was held that:

> "The recording of a private conversation without the knowledge of the participants or one of those participants is an interference with their private life, which is protected by Article 8 of the Convention".[43]

In the light of this, it should not matter how the conversation is recorded. Furthermore, to be compatible with Article 5 of the Directive, which RIPA implemented, the confidentiality of the communications must be protected.

It was argued in *R v. E* that as the protection called for by the Directive extended to protection against listening storage and surveillance of communications, a fresh approach to the construction of the word "interception" as used in RIPA, was needed.[44] The Court cited Recital 12 and Articles 3 and 14 of the Directive which expressly permits measures judged necessary in Member States for the enforcement of the criminal law. The Court also pointed to Part 11 of RIPA which contains a complex of rules requiring surveillance in different forms to be regulated and that included the surveillance of communications. Under section 48 of RIPA, surveillance clearly includes the monitoring of conversations, telephone or otherwise.

Neither Article 8 nor the Directive require more than the regulation of interference with communications; they do not require that lawfully obtained material should be inadmissible at a criminal trial. There was therefore no need for "interception" to be redefined so as to be compatible with Article 8 or the Directive.

Should all authorisations for intercepts be placed in the hands of the judiciary? Is this more likely to meet ECHR requirements? Is the degree of scrutiny sufficient? Surveillance authorisations which may include the interception of communications can be issued by superintendents or inspectors.[45] This, arguably, relegates the importance of the caller's privacy rights.

## Conclusion

A blanket prohibition on the use of intercept evidence is hard to justify. There ought to be some relaxation which allows the prosecution to adduce intercept evidence. At the moment such material remains open to doubt and criticism as to its quality, in particular as a basis for house arrest. Incarcerating suspects on the strength of such material is but a step away.

The Government is under considerable pressure to ease the prohibition on the evidential use of intercept material. The Metropolitan Police Commissioner, the Joint Parliamentary Committee on Human Rights, the Director of Public

Prosecutions and Liberty have all spoken out against this prohibition. Given this pressure and the absence of a similar prohibition in most countries, it will be interesting to see how long the Government maintains this hard line stance.

1 RIPA 2000, Explanatory Notes, 1, para 3.
2 *Halford v. United Kingdom* [1997] 24 EHRR 523.
3 RIPA 2000, section 2(1).
4 RIPA, sections 5-11 and 15.
5 *A-G's Reference No. 5 of 2002* [2004] UKHL 40, para 9.
6 Code of Practice on Interception of Communications, TSO (2002), s.10.1.
7 RIPA 2000, Explanatory Notes, 5, para 24.
8 *R. (NTL Group Ltd) v. Crown Court* at Ipswich [2003] Q.B. 131, DC.
9 RIPA 2000, Explanatory Notes, 7, para 39.
10 RIPA 2000, Explanatory Notes, 8, para 40.
11 Code of Practice on *Interception of Communications*, TSO (2002), s.10.2.
12 *www.dti.gov.uk/cii/regulation.html*.
13 RIPA 2000, Explanatory Notes, 10, paras 55 and 56.
14 RIPA 2000, Explanatory Notes 11, para 59.
15 RIPA 2000, 6, para 32.
16 Lord Bassam during the Committee stage of the Bill in the House of Lords.
17 April 23, 2002, Woolwich CC.
18 D. Ormerod and S. McKay, "Telephone intercepts and their admissibility"[2004], Crim L.R. 24.
19 RIPA Pt II.
20 Hardy and Hardy [2003] Crim.L.R. 394.
21 [2002] EWCA Crim. 1243.
22 [2004] EWCA Crim 1243.
23 [2002] EWCA Crim 772.
24 [2005] EWCA Crim 703.
25 Cm.4368,1999, paragraph 4.5 of the Consultation Paper.
26 February 7, 2005: House of Commons debates.
27 RIPA 2000, Explanatory Notes, 21.
28 RIPA 2000, Explanatory Notes, 21.
29 Code of Practice on *Interception of Communications*, TSO (2002), 25.
30 [2003] EWCA Crim 1632.
31 [2004] UKHL 40.
32 D. Ormerod and S. McKay, "Telephone intercepts and their admissibility" [2004] Crim.L.R. 34.
33 D. Ormerod and S. McKay, "Telephone intercepts and their admissibility" [2004] Crim.L.R. 31.
34 ibid, 31.
35 Para 9 of the Home Office RIPA Explanatory Notes (2000).
36 *Kruslin v. France* [1990] 12 E.H.R.R. 528, para 26; *Valenzuela Contreras v. Spain* [1999] 28 E.H.R.R. 483, para 75; *Huvig v. France* [1990] 12 E.H.R.R. 528; *Kopp v. Switzerland* [1999] 27 E.H.R.R. 91, para 72.
37 *Malone v. UK* [1984] 7 E.H.R.R. 14; *Halford v. UK* [1997] 24 E.H.R.R. 523; *Khan v. UK* [2001] 31 E.H.R.R. 45.
38 *Hammond, McIntosh and Gray* [2002] EWCA Crim.1243.
39 D. Ormerod and S. McKay,"Telephone intercepts and their admissibility" [2004] Crim.L.R. 21.
40 See note 18.
41 *MacDonald*, April 23, 2002.
42 *Halford v. UK.*
43 [1993] 17 E.H.R.R. 462, para 34.
44 [2004] EWCA Crim 1243.
45 RIPA s. 1(5) (c) and .48(4).

# Germany: Impact of the E.U. Standard Contractual Clauses on the Use of Data Processors Outside the EEA

*By Dr. Christoph Rittweger and Dr. Michael Schmidl, Partner and Associate, respectively, in the Information Technology Group of Baker & McKenzie LLP, Munich. Dr. Schmidl is a lecturer in Internet law at the University of Augsburg.*

According to the German Federal Data Protection Act ("BDSG") the transmission of personal data from a German data controller to a data processor located *within the European Economic Area* is not treated as a "transfer" ("Übermittlung") within the meaning of the BDSG. This follows from section 3 (8) BDSG, which stipulates that a data processor located in Germany, or in another Member State of the European Union or in another state being party to the Agreement on the European Economic Area ("EEA") does not qualify as a "third party" within the meaning of the BDSG. Accordingly, a data processor within the EEA is to be treated as if he was part of the controller and the controller therefore must not meet the statutory prerequisites for the admissibility of data transfers according to section 4(a), 28 subseq. BDSG. On the contrary, the data controller's only obligations when using a data processor within the EEA are exclusively governed by section 11 BDSG, which stipulates merely that the data controller needs to:

- carefully select the processor;
- ensure that the processor adopts the required technical and organisational measures (section 9 BDSG); and
- sign a written order according to which the data processor will only process personal data received from the data controller in accordance with the instruction received from the data controller.

The transmission of personal data from a German data controller to a data processor located *outside the European Economic Area* is treated as if it were a transfer of personal data between two controllers and thus the prerequisites for an international transfer of data under the BDSG need to be met.[1] This equally follows from section 3(8) BDSG, which – as explained above – treats a data processor outside the EEA as "third party" within the meaning of the BDSG, regardless of whether such data processor is bound by way of the standard contractual clauses for the transfer of personal data to processors in third countries pursuant to Directive 95/46/EC (the "Standard Contractual Clauses").[2]

For transfers of personal data to countries outside the EEA, the BDSG generally requires a two-step test, which the German data controller would need to meet with in order to make legal use of a data processor outside the EEA. The

first step deals with the question of whether an adequate level of data protection within the meaning of Directive 95/46/EC ("Directive") exists at the recipient's end. This step will undoubtedly always be met when the data processor is bound by unmodified Standard Contractual Clauses. The second step requires that the statutory prerequisites for a transfer between two parties are met in accordance with sections 4(a), 28 subseq. BDSG. The second step thus either requires:

- the data subject's consent to the transfer (which the data controller in most instances will not seek for reasons of practicality);
- the necessity of the transfer to fulfil the contractual obligations of the controller vis-à-vis the data subject (this criterion will be difficult to meet since the use of a data processor is generally never necessary to fulfil the data controller's contractual duties vis-à-vis the data subject); or
- a justified interest of the data controller to transfer the data to the data processor outside the EEA and no overriding interest of the data subject.

The question, which therefore arises, is: What effect does the use of the Standard Contractual Clauses have for the second step of the two-step test under German law? Or rather: Does the use of a processor outside the EEA safeguard justified interests of the controller and does the data subject have no overriding interest if the data controller binds the data processor by way of the Standard Contractual Clauses? Or summarised in practical terms: Is a data processor located outside the EEA to be treated the same as a data processor located within the EEA if the data processor outside the EEA is bound to the level of data protection of the European Union by way of the Standard Contractual Clauses?

The following aims to answer these questions both with regard to "normal" personal data and also with regard to "sensitive data", based on the assumption that the relevant data subjects have not consented to the transfer of their personal data to the data processor.

## Admissibility of the Transfer Pursuant to Section 28 BDSG

### "Normal" Personal Data

According to section 28(1)(2) BDSG, the German data controller would need to establish that the transfer of "normal" personal data to the data processor outside the EEA "is necessary to safeguard justified interests of the controller and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use". According to German legal commentators, a justified interest of the data controller can generally be assumed if "there is no proper and reasonable alternative" for the measure envisaged. The question thus arises whether the use of a data processor within the EEA (which would always be legally permissible if the prerequisites of section 11 BDSG were met) would qualify as "proper and reasonable alternative". If this were the case all processing of personal data by data processors would have to be carried out exclusively by processors within the EEA. Such a restrictive interpretation of section 28 (1)(2) BDSG would directly contradict the "effet utile" of the EC Commission's decision on Standard Contractual Clauses since it was the EC Commission's intention to allow the use of data processors established outside the EEA. Such intention is binding for the Member States pursuant to article 249 subsection 4 of the EC Treaty.[3] A restrictive administration of section 28 (1)(2) BDSG, which would – as demonstrated – result in the virtual prevention of international commissioned data processing, is thus to be considered in light of European law.

Taking this into consideration, the data controller's justified interests to use a data processor outside the EEA cannot be denied simply on the basis that a data processor within the EEA could perform the same tasks as well. When it comes to the balancing of interests between the data controller on the one hand and the data subjects' on the other, one rather has to consider the criteria directly manifesting the interest in the data processing of the controller and possible legitimate overriding interests of the data subjects'. Possibly justified interests for the data controller could for example stem from the fact that the data processor outside the EEA is cheaper than data processors within the EEA or from the fact a group member outside the EEA is commissioned with the data processing for all group companies thus making it more convenient and possibly also more secure to process all the data at one location. Thus any kind of legal, economic or idealistic interest of the data controller to use a data processor outside the EEA should be recognised as qualifying as justified interest within the meaning of section 28(1)(2) BDSG.

Once it has been confirmed that the data controller has justified interest in using a data processor outside the EEA, the second question arises of whether there is reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use. Within the scope of the balancing of the interests of the data controller and of the data subject that is required in this context, the similarity of the data processor within the EEA with the data processor outside the EEA who is bound by E.U. data protection standards by means of the Standard Contractual Clauses has to take effect. The statutory judgment that a transmission of data to a data processor within the EEA does not qualify as a transfer within the meaning of the BDSG, due to the effect that all EEA members provide for an adequate level of data protection, must thus be taken into consideration within the scope of the balancing of interests in favour of the data controller. Even in the event that one could not – as would be desirable – arrive at full legal equality of the non-EEA and the EEA data processor, it is still necessary to bring the non-EEA commissioned data processing closer to internal EEA commissioned data processing, at least by way of a liberal interpretation of the permission standards, in order to respect the "effet utile" of the decision by the Commission in the manner described above.

Section 28 BDSG should therefore cause the non-EEA commissioned data processing as regards to "normal" personal data on the basis of Standard Contractual Clauses to fail in exceptional cases only.

## Sensitive Data

The result must be the same when it comes to the use of Standard Contractual Clauses in connection with

 

sensitive data ("special categories of personal data" within the meaning of section 3(9) BDSG and the Directive) as well.

The prerequisite (the second step of the two-step test mentioned above) for transferring sensitive data are set forth in section 28(6) – (9) BDSG which only allow for the transfer of sensitive data in very limited circumstances which will typically not be readily available when using a data processor for such data. When applied to data processors outside the EEA, section 28(6) – (9) BDSG is therefore also likely to be contrary to the "effet utile" of the decision by the EC Commission on the Standard Contractual Clauses, since like the rest of section 28 it does not provide for any exemption which would take into account the creation of an adequate level of data protection between the data controller and the data processor.

The existence of Clause 4f of the Standard Contractual Clauses makes it very clear that the EC Commission wanted to allow the processing of sensitive data by processors located outside the EEA. Clause 4f of the Standard Contractual Clauses declares it to be sufficient that the data subject has been informed or will be informed of the processing of his sensitive data by the data processor outside the EEA. An application of section 28(6) – (9) BDSG strictly following the wording would thus cause the EC Commission's decision to be meaningless. Such interpretation of German law would not be justified under European law. If, as with "normal data", an adequate level of data protection is established by using Standard Contractual Clauses, there is no longer a basis for making distinctions between data processors within the EEA and those outside the EEA.

In summary, the use of data processors outside the EEA also has to be admissible in case of sensitive data. The geographic location of the data processor as a criterion for making a distinction as set forth in the Directive and the BDSG has been eliminated by way of the creation of an adequate level of data protection within the relationship between the data controller and the data processor. The continuing discrimination of non-EEA data processors is not justified under European law.

## Summary

German data protection law (the BDSG) treats the use of data processors differently depending on whether the data processor is located within or outside the EEA. Whereas a German data controller using a data processor within the EEA does not need to comply with the rules on data transfers established under the BDSG, a data controller using a data processor outside the EEA will need to comply with such transfer rules.

The German transfer rules for transfers to countries outside the EEA consist of a two-step test. The first step according to which there must be an adequate level of data protection for the recipient located in a non-EEA country will be met by signing the Standard Contractual Clauses between the data controller and the data processor. The second step of the test in most circumstances will depend upon whether the German data controller has justified interests for using the processor outside the EEA and whether the data subject has an overriding interest to prevent the processing of its data by the data processor outside the EEA.

Since the German legislator does not consider the transmission of data to a data processor within the EEA to be a transfer within the meaning of the BDSG and consequently does not regard the commissioned data processing as potentially endangering the data subject, the same should apply in respect to data processors outside the EEA which are bound by the Standard Contractual Clauses. The use of Standard Contractual Clauses eliminates the inadequate level of data protection as a criterion for making a distinction between EEA and non-EEA data processors. Under normal circumstances the balancing of interests between the controller's and the data subjects' interests should therefore be decided in favour of the data controller, always provided the controller can show some kind of idealistic, financial, security or other interest in using a data processor outside the EEA and there are no exceptional circumstances which would warrant the interests of the data subject overriding those of the controller.

Given the fact that the Standard Contractual Clauses expressly mention the processing of sensitive data, the same should apply to the processing of sensitive data by data processors outside the EEA which are bound by the Standard Contractual Clauses.

1 This is in line with the Commission's intention that the standard contractual clauses are (only) supposed to be to the effect that the Member States have to acknowledge the obligations of data exporter and data importer contained in the standard contractual clauses as appropriate safeguards. In the relevant decision the Commission clarifies that the transfer of personal data to a data processor resident outside the EU/EEA constitutes an international data transfer which is protected by Chapter IV of Directive 95/46/EC. Article 2 subsection 1 sentence 2 of the decision contains an explicit provision to that effect which makes reference to the validity of the national data protection provisions created in implementing the Directive.

2 Decision 2002/16/EC by the Commission dated December 27, 2001, with respect to standard contractual clauses for the transfer of personal data to processors in third countries pursuant to Directive 95/46/EC.

3 In this context cf. Streinz-Schroeder, article 249 EGV, fn. 138.

*The authors wish to thank Mr. Andreas Lickleder (Rechtsanwalt) for his support with this article.*

# Guidance on Privacy and Consent in Canada

*By Elizabeth McNaughton, Ian Hay and Veera Rastogi, Blake, Cassels & Graydon LLP. The authors are Partner and Associates, respectively, in the Toronto office of Blakes and may be contacted at elizabeth.mcnaughton@blakes.com; ian.hay@blakes.com and veera.rastogi@blakes.com*

The first detailed substantive decision of an appeal court on Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) provides important comments on a number of issues under Canadian privacy legislation. The initial complaint before the federal Office of the Privacy Commissioner (the Commissioner) involved the type of consent required under PIPEDA for the listing of first-time customers' personal information in telephone directories, the appropriate manner of obtaining that consent, and the reasonableness of fees charged for de-listing. In the subsequent proceedings in the Federal Court and the Federal Court of Appeal, the courts considered a number of additional issues, including interpretation of PIPEDA, the nature of hearings under PIPEDA and deference to the Commissioner, the standing of complainants and jurisdictional issues.

This article focuses on the Court's comments on the type of consent required to meet PIPEDA's "knowledge and consent" standard and the Court's comments on the deference, or lack thereof, to be paid to decisions of the Commissioner. On both of these issues, the Court of Appeal reversed the decision of the lower court and disagreed with the earlier findings of the Commissioner.

## Consent

A major Canadian telecommunications provider had tried to obtain consent from first-time customers by having its customer service representatives indicate to customers that subscription to a new telephone line includes a listing in its directory. Customers were then asked how they would like their personal information to appear in the directory. If a customer expressed an interest in not having his or her name published in the directory, options, including the ability to opt out of the directory listing, were discussed only at that point. Once a customer had enrolled, they received written material including a privacy brochure that set out the purposes for the collection, use and disclosure of their personal information and of their right to be de-listed.

The lower court found that the company and its affiliates use and disclose customers' names, addresses and telephone numbers not only to publish its directory, but also for a number of secondary purposes, including dial-in and Internet directory assistance as well as the licensed sale of the information as a retail product in CD-ROM format. While these purposes are outlined in the privacy brochure sent to customers following enrolment, they are not identified at the time customers initially call to subscribe to a new telephone line. However, the lower court reasoned that first-time customers would be well aware of the established practice of telephone companies to include directory listings as part of their residential telephone services and that, as such, the company could assume that it had their implicit consent in this regard unless customers specifically requested an unlisted number on their own initiative at the time of enrolment.

The Court of Appeal overturned the decision of the lower court on the consent issue, finding that the company had infringed PIPEDA in two respects. First, it had failed to inform first-time customers, at the time of enrolment, of the secondary purposes for which their personal information is used and disclosed. On this point, the Court of Appeal held that: "These services were not identified at the time of enrolment and there is no evidence that they were so connected with the primary purposes of telephone directories that a new customer would reasonably consider them as appropriate. There is no evidence that TELUS made any "effort", let alone a "reasonable" one, within the meaning of clause 4.3.2, to ensure that its first-time customers are advised of the secondary purposes at the time of collection."

The Court of Appeal found that the company had also infringed PIPEDA in not informing customers, at the time of subscription, of the availability of the Non-Published Number Service (NPNS), finding the position of the lower court on implied consent to be incompatible with the very requirement of seeking the knowledge and consent of customers at the time of collection, as mandated by Part I and Schedule I of PIPEDA. The Court of Appeal stated that "[a] consent is not informed if the person allegedly giving it is not aware at the time of giving it that he or she had the possibility to opt out". In the Court's view, it was particularly important in these circumstances that customers immediately be made aware of their right to subscribe to the NPNS, as personal information published in a telephone directory becomes "publicly available" under PIPEDA regulations with the consequence that it can be further used and disclosed without consent. The Court asserted that only with such knowledge and consent can effect be given to the express purpose of PIPEDA, which is to strike a balance between individuals' right to privacy and industry's need to collect, use and disclose personal information for appropriate purposes.

## Deference to the Privacy Commissioner

On the issue of the deference to be paid to the Commissioner, the lower court in this and previous decisions had indicated that the report of the Commissioner was "entitled to some deference with respect to decisions clearly within his jurisdiction". The Court of Appeal appears to reject this view. Previous Federal Court decisions have confirmed that a hearing under section 14 of PIPEDA is a proceeding *de novo*, or a new action. However, the Court of Appeal went further and concluded that, because the nature of the proceeding is not a review of the Commissioner's report per se but a review of the conduct of the respondent company, the report of the Commissioner may be contradicted or challenged like any other document put in evidence and was not entitled to any deference. The Court of Appeal reasoned that, because PIPEDA provides that the Commissioner may appear as a party at the court hearing, showing deference to the Commissioner's report would compromise the fairness of the court hearing.

  WDPR ISSN 1473-3579

## What is the Impact of this Decision?

Of particular significance to businesses is that the Court of Appeal interprets PIPEDA to *require* organisations to identify to individuals all purposes for the collection, use and disclosure, as well as any opt-out options, *at or before the time of collection*. On its face, this requirement, in terms of the timing of the identification of purposes and consent options, affords organizations less leeway than comments of the current federal Privacy Commissioner in recent speeches or even the wording of the "Identifying Purposes" and "Consent" principles in Schedule 1 of PIPEDA. It is possible that this interpretation may have been informed by the particular facts of this case, given that the consequence of a directory listing is that the information becomes publicly available. However, until this issue is considered by the Court on different facts, and particularly in light of the Court's finding on the issue of deference to the Commissioner, it is at least arguable that the Court of Appeal has raised the bar on the "knowledge and consent" requirement of PIPEDA.

# France: Data Retention Obligations for Employers Providing Internet Access to Staff

*By Karin Retzer and Cyril Ritter, Morrison & Foerster, Brussels. The authors may be contacted at kretzer@mofo.com and critter@mofo.com*

The 1997 Telecommunications Privacy Directive[1] provided that E.U. Member States[2] had the possibility, but not the obligation, to require telecom operators to retain communication data arising out of the use of the telecommunications system for law enforcement purposes. That Directive was replaced by the 2002 Electronic Communications Directive[3] in order to adapt the E.U. legal regime to technical developments such as the growth of the Internet. The new Directive extended the scope of the 1997 Directive by explicitly allowing E.U. countries to compel telecom and Internet service providers (ISPs) to record and store traffic data under certain circumstances. National laws must, however:

- ensure that the data are only retained for a limited period of time;
- aim to achieve specific, enumerated "public order" purposes;
- be necessary, appropriate, and proportionate within a democratic society for achieving these purposes; and
- be consistent with the European Convention on Human Rights. The Directive fails to regulate the time period for which the data must be retained.

Since then, a battle has emerged between, on one side, Member State law enforcement and intelligence agencies, who are pushing for the retention of all communication data, and, on the other side, privacy advocates and ISPs, who strongly resist these demands. At the International Data Protection Conference in Cardiff in September 2002, data protection and privacy commissioners expressed "grave doubts as to the legitimacy and legality of such broad measures."[4] Also, the Article 29 Working Group, which is an advisory body made up of the national data protection authorities of the 25 E.U. Member States, has issued highly critical position papers, arguing that broad data retention schemes conflict with one of the core principles of E.U. data protection law, the proportionality principle under which the amount of data collected is limited to what is necessary to achieve the purpose(s) for which the data are gathered. Data must also be erased when no longer needed for the specific purposes for which they were collected. However, questions relating to the breadth of the regime and the concerns about the invasion of personal privacy, the sheer magnitude of the volume of data, and the considerable costs involved remain largely unresolved.

A legal issue that employers throughout Europe have been facing is whether they would also become subject to the same obligations when they make internet access available to their employees. This is the question that was squarely presented to the Paris Court of Appeal (*Cour d'Appel de Paris*, "Court") in *BNP Paribas v. World Press Online*.[5] The judgment was delivered on February 4, 2005.

## Facts

World Press Online ("WPO") is a U.S.-based online press and photo agency. In 2004, two of WPO's business partners received anonymous e-mails alleging that WPO was on the brink of bankruptcy. These e-mails appeared to have been sent in 2003 from a Yahoo! e-mail account which was accessed from a France-based computer located in the offices of BNP Paribas ("BNP"), one of the leading French banks.

Alleging that these two business partners had subsequently severed business links with the company as a result of receiving these e-mails, WPO requested assistance from BNP in order to determine the identity of their author. Faced with BNP's refusal to cooperate, WPO sought a court order compelling BNP to provide the name of the author of the allegedly illegal and malevolent e-mails on the basis of the relevant communication data. The order was eventually granted by the Paris Commercial Court (*Tribunal de Commerce de Paris*) in October 2004.

On appeal, BNP argued that obligations to protect employee privacy prevented it from retaining the communication and turning over the information. The bank also argued that data retention obligations were devised as part of the legal framework for ISPs, not to create new, costly data retention obligations for all employers providing internet access to their employees.

## Key Holding

The Court held that while there was no legal obligation on BNP to actually identify the author of the allegedly illegal e-mails, BNP was under an obligation to retain and hand over all relevant traffic data. (As a practical matter, it is conceivable that the traffic data may make it possible to identify the individual employee authoring the e-mails. Then again, depending on its internal configuration, identifying the author may require BNP's cooperation.)

Ruling on the traffic data issue, the Court referred to the 1986 "Liberty of Communications Act (*Loi relative à la liberté de communication*)[6] as amended in 2000 ("Communications Act"), to provide for the mandatory retention of certain types of internet data. The Court found that the Communications Act makes no distinction between ISPs who offer Internet access on a commercial basis, and employers who give internet access to staff.

## Comment

Sadly, the Court's judgment does not contain any legal reasoning leading to this interpretation. Nor does it consider BNP's argument that on a proper reading of the Communications Act, employers should not be held to the same standard as ISPs in terms of data retention. It is unfortunate that the Court did not explore the preparatory works of the 2000 amendment to the Communications Act, which lend strong support to BNP's legal reasoning. Draft versions of the 2000 amendment to the Communications Act as well as the *Assemblée Nationale* and *Senate* reports state that data retention obligations apply to ISPs and web hosting providers. Furthermore, it is clear from the legislative history of the 2000 amendment that the data retention provisions were aimed at counterbalancing another provision in the same amendment according to which ISPs are largely shielded from liability for content (*e.g.*, pictures, news stories, websites, *etc)*. Since ISPs are largely protected from lawsuits related to "content," it was considered fair to require them to provide traffic data in order to identify "content" providers, so that aggrieved parties can effectively bring lawsuits against the original "content" providers. Clearly, it was never the intention of the French legislature to include all employers generally within the scope of the data retention obligation.

In view of this judgment and upcoming legal developments, it seems that the issue of mandatory retention schemes for communication data (and the corresponding requirement to invest in equipment and technological expertise) is becoming both confusing and unavoidable, at least in France where data retention obligations on ISPs and, possibly, employers are governed by a patchwork of overlapping legal provisions. The Communications Act, the "Law on Everyday Security" (*Loi sur la Sécurité Quotidienne*) of 2001[7] and the "Law on Confidence in the Digital Economy" (*Loi pour la Confiance dans l'Economie Numérique*) of 2004[8] all contain provisions on traffic data retention. Both the Communications Act and the "Law on Confidence in the Digital Economy" provide for a general obligation to retain traffic data. Both laws provide that the details should be worked out in implementing decrees, which have not yet been adopted. Under the "Law on Everyday Security," the position is that there is a derogation "for the purpose of" law enforcement from the general obligation under the proportionality principle to limit the amount of data collected and retained to what is strictly necessary to achieve the purpose(s) for which the data are gathered. Again, no further details are provided. Yet another implementing decree is due to be adopted on the basis of the "Law on Everyday Security." For the moment, ISPs and, according to the Court, employers are left in legal limbo.

One reason that might explain the delay in adopting implementation legislation in France is that there are developments at the E.U. level. In April 2004, a number of Member States, including France, Ireland, Sweden, and the United Kingdom, tabled a draft decision[9] on the retention of telecom/Internet traffic data for the purpose of criminal law enforcement (including counter-terrorism). They cited the March 2004 bombings in Madrid as illustrating the necessity to better control such data. Although this draft decision has met with considerable criticism within the Article 29 Working Group[10] and in the French Senate, ISPs and employers can expect extensive regulation and onerous obligations resulting from these movements, as they are consistent with a broader trend towards tighter legal control over the internet. From this point of view, it could be argued that the *BNP v. WPO* judgment merely gives them a taste of what lies in store for them.

1 Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24/1 of January 30, 1998.

2 The 25 Member States of the European Union currently are: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, the Netherlands, and the United Kingdom.

3 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201 of July 31, 2002, p. 37.

4 See *www.fipr.org/press/020911DataCommissioners.html*.

5 See *www.foruminternet.org/telechargement/documents/ca-par20050204.pdf*.

6 See *www.assemblee-nationale.fr/ta/ta0553.asp*. The 2000 amendment amends articles 43-7 to 43-9 of the 1986 Communications Law.

7 See *www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX0100032L*.

8 See *www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=ECOX0200175L*.

9 Council document 8958/04, presented on April 28, 2004 (plus addendum of December 20, 2004), at *http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf* and *http://register.consilium.eu.int/pdf/en/04/st08/st08958-ad01.en04.pdf*. The European Commission subsequently issued a consultation document on this topic. See *http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/public_consult/data_retention/consultation_data_retention_30_7_04.pdf*.

10 See Opinion 9/2004 adopted on November 9, 2004 at *http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp99_en.pdf*.

 

# Germany: New Proposals to Counter Spam

*By Kerstin A. Zscherpe and Andreas Splittgerber, Baker & McKenzie LLP, Frankfurt/Munich*

On February 17, 2005, the ruling German coalition parties introduced a bill (*BT-Drucksache 15/4835*) to the Parliament (*Bundestag*) aiming to better counter the spread of unsolicited commercial e-mails ("Spam"). Under current German law – and in accordance with the European Directive on privacy and electronic communications (2002/58/EC) – such unsolicited e-mails constitute an infringement of the newly amended section 7 of the Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*) if they are sent without the prior consent of the recipient and without the relevant sender identification. When such e-mails are illegally sent, competitors are entitled to launch injunctions, abatement claims as well as civil claims for damages and the surrender of the profits made as a result of the Spam. In addition, consumers associations and certain other organisations are also entitled to launch injunction actions. These legal instruments are now to be supplemented by the possibility of public authorities to intervene against the Spam sender. The corresponding right of action shall arise from the Teleservices Act (*Teledienstegesetz – TDG*), a statute aimed at regulating certain aspects of dealings in the Internet. The Bill provides that the sending of Spam constitutes an administrative offence, subject to a fine, when the commercial character and/or the sender of the e-mail has been disguised or concealed.

## Content of the Bill

The Bill provides for the introduction of a new subparagraph 3 to section 7 of the TDG. In terms thereof it shall not be permitted to disguise or conceal the sender and/or the commercial character of the e-mail in the header and/or subject line. The disguising and/or concealment will be deemed to have occurred when, prior to opening the mail, the recipient receives no or only misleading information concerning the sender's identity or the commercial character of the e-mail (section 7(3)(2) of the TDG Bill). A violation of this prohibition will, in terms of the planned section 12(1)(2) of the TDG Bill, lead to a possible fine of up to €50,000.

According to the Bill, not only the direct senders of Spam e-mails will be subject to a fine, but the person who ordered and/or assisted the sending of such e-mail will also be liable in this regard. It is, however, intended that the Bill will not apply in cases where the sender does not intend to disguise or conceal his identity and/or the commercial character of the e-mail, in particular because the sender, due to lack of knowledge, merely failed to draft the e-mail clearly.

## Consequences of the Proposed New Rules

If the Bill were adopted in its present form, this would mean that, in the composition of a commercial e-mail, the commercial character as well as the sender must be made clear in the header and subject line of the e-mail. Therefore, it is no longer acceptable that the recipient is only able to ascertain the relevant information from the contents of the e-mail. In terms of the Bill, every recipient must be able to identify from the header and subject line alone who the sender of the e-mail is and that the message concerned is an advertisement.

It can, therefore, be assumed that the following examples will be misleading and therefore prohibited:

- the composition of an e-mail so as to give the recipient the impression that the e-mail was sent from his circle of friends, from a government agency or from a business partner; or
- including false IP addresses in the sender information in the e-mail; or
- the substitution of the recipient's address as that of the sender's.

Further, the sender is not permitted to conceal his identity by:

- failing to include an address in the sender line of the header; or
- sending the e-mail without a header; or
- making the e-mail anonymous through the use of a re-mailer.

In addition, the following examples of common subject line practices are not permitted:

- giving the impression the e-mail is urgent; or
- using an apparent personal address in order to persuade the recipient to open the e-mail; or
- indicating that the e-mail is a response to a prior e-mail sent by the recipient.

Failure to comply with the new requirements can lead to significant fines of up to €50,000. It is, however, unclear what the subjective requirements are for a sender. The lack of clarity derives from the paradox that while section 7(3)(2) of the TDG Bill requires that the sender must act with express intent, section 12(1)(2) of the TDG Bill states that both negligent and intentional acts suffice for an administrative offence. Thus, it seems that the provisions are contradictory. However, since the use of the words "in particular" in section 7(3)(2) of the TDG Bill indicates that the provision only seeks to provide example and non-limiting definitions of the terms "disguise" and "conceal", it can be potentially assumed that negligent acts are already prohibited and, thus, subject to administrative fines. The authors of the Bill have, however, taken the position that the proposed rules will not apply to negligent behaviour, for example where a business fails to sufficiently comply with the statutory provisions. In the interest of legal certainty, it is desirable that the future legislative steps will rid the Bill of the contradictions.

## Further Proceedings

Generally, it still has to be seen if and to what extent the Bill will be changed in the further legislative process. Still unsolved – and perhaps unsolvable – is the problem that many Spam senders operate from outside of Europe and that the implementation of any national rules will be subject to enforcement difficulties.

In addition, the planned new rules only refer to e-mail communications, leaving other communication methods such as instant messaging and short message services absent from legal protection.

# Freedom of Information: Contractual Consultation Obligations

*By Richard Best, Ashurst, Frankfurt. The author may be contacted on tel. +49 69 9711 2757 or at richard.best@ashurst.com*

It is well known that the U.K. Freedom of Information Act 2000's right of access to information held by public authorities came into force on January 1, 2005. It is also known that commercial entities dealing with or otherwise providing information to public authorities could be affected by the changes. For example, individuals, competitors, journalists or potential claimants may request and sometimes obtain commercially sensitive information originally supplied by those entities.

Public authorities transacting with such entities are likely to find that contractual negotiations include a request for inclusion of a clause requiring consultation prior to disclosure under the Act. Questions may arise as to what liabilities a public authority could face if it were to breach that clause, given that the circumstances surrounding such a breach would usually entail the public authority's compliance with a statutory duty to disclose information to the requesting party. Could a public authority find comfort in the notion that compliance with that statutory duty might trump a contractual obligation and therefore exclude contractual liability? In all likelihood, the short answer is no and that a failure to comply with a contractual consultation clause may render the authority liable for damages. This article considers this issue by reference to relevant New Zealand case law under that country's Official Information Act 1982.

## Consultation as a Prerequisite to Disclosure under the Freedom of Information Act ("FOIA")

Where an authority is in doubt as to whether its disclosure would constitute a breach of confidence, or might otherwise fall under an exemption, it can be expected to consult with the party from whom the information was obtained. To some extent this issue is now covered in the Secretary of State's Code of Practice on the Discharge of Public Authorities' Functions Under Part I of the Freedom of Information Act 2000 (the "FOIA Code") as revised in November 2004.[1]

The FOIA Code states that in some cases it will be necessary to consult, directly and individually, with third parties to determine whether or not an exemption applies to information requested, or to reach a view on whether the Act's disclosure obligations arise in relation to that information. It also states that in a range of other circumstances it will be good practice to do so: "for example where a public authority proposes to disclose information relating to third parties, or information which is likely to affect their interests, reasonable steps should, where appropriate, be taken to give them advance notice, or failing that, to draw it to their attention afterwards." The Code states further that it may also be appropriate to consult third parties about matters such as whether any further explanatory material or advice should be given to the applicant together with the information in question. Such advice may, for example, refer to any restrictions (including copyright restrictions) which may exist as to the subsequent use which may be made of such information.[2]

One may note that the FOIA Code's expectation of consultation "in some cases" is neither precisely defined nor statutory in nature.[3] One might argue on public law grounds that consultation is mandatory where confidential or commercially sensitive information is at stake, but these arguments, although strong, are not necessarily robust.[4] Perhaps more importantly, breach of a public law obligation does not, without more, give rise to an action for damages against the public authority. For these reasons, companies transacting with public authorities may wish to include contractual consultation clauses to ensure, to the extent one can, that their counterparty public authorities will be subject to a contractually binding obligation to consult. For example, they may want to include a term stating that no confidential information shall be disclosed except where:

- the public authority has consulted the other contracting party on the proposed disclosure or at least reasonably informed that party of the proposed disclosure (within, for example, 7 days of receipt of a request, to enable that party to respond); and
- disclosure is required by law, under FOIA or otherwise.

## Are Such Clauses Binding? The Astra Pharmaceuticals Case

If properly drafted, this kind of clause ought to enable companies to protect their commercial position as best they can prior to the proposed disclosure. Such clauses have been employed in other jurisdictions with freedom of information legislation, perhaps most notably, from the perspective of case law on their validity, in New Zealand.

The key case is *Astra Pharmaceuticals (NZ) Limited v. Pharmaceutical Management Agency Limited.*[5] The Pharmaceutical Management Agency ("Pharmac") is New Zealand's regulatory body responsible for determining which pharmaceutical products are subsidised from public funds. It frequently enters into contracts with suppliers setting out the terms on which their products will be subsidised. In this case, Astra Pharmaceuticals had entered into such a contract for its anti-ulcerant drug Losec (a proton pump inhibitor ("PPI")). It sued and sought damages from Pharmac for breach by Pharmac of the confidentiality obligations in that contract.

Prior to the contract, the PPI therapeutic subgroup, to which reference pricing had been applied (the effect of which is to subsidise each product in the subgroup at a level equating to the price of the lowest priced product), consisted of Losec and Zoton. To limit expenditure across the anti-ulcerant therapeutic group (which consisted of the PPI subgroup and an H2 antagonist subgroup ("H2As")), Pharmac had placed restrictions on subsidisation of drugs in the PPI subgroup to the extent that they were only subsidised if the patient had first been treated with H2As, had seen a specialist, and had an endoscopy. Astra wanted these restrictions lifted.

  WDPR ISSN 1473-3579

In October 1997 Pharmac agreed to lift the restrictions in return for Astra's agreement to reduce the average daily cost ("ADC") of the drug (which, through reference pricing, automatically lowered the level of public subsidy for all drugs in the PPI sub-group) and to guarantee a cap on the level of total Pharmac expenditure across the entire anti-ulcerant therapeutic group. The contract provided that, in general, reference pricing should continue, but there would be an exemption from the reference pricing system where any reduction in the ADC of Losec's subgroup was the outcome of a cross deal by Pharmac with another company.

Importantly for present purposes, the Losec contract also contained a confidentiality clause in respect of information each party provided to the other in the course of negotiating the contract. Under that clause, a prerequisite to disclosure, even under the Official Information Act 1982 (NZ) (similar to FOIA), was that "the other party ha[d] been reasonably informed prior to any such disclosure". In addition, Pharmac could not disclose the information "for the purposes of consultation [in relation, for example, to other subsidisation proposals] unless it [had] consulted with [Astra] before releasing that information."

Although, as part of its consultation process with the industry, Pharmac disclosed to Astra's competitors that Losec was to be de-restricted and that Astra had agreed to lower the ADC of Losec and manage an expenditure cap across the anti-ulcerant group, the Court's judgment states that the fact that there was an exemption from reference pricing was not disclosed.

Subsequently, and albeit after initial refusal to a request under the Official Information Act which was taken to the Ombudsman, Pharmac disclosed details of the Losec agreement to another company, Pharmacia and Upjohn ("P&U"), whose competing PPI (Somac) had also been listed on the Pharmaceutical Schedule (meaning it too was authorised to be state funded). P&U then made a proposal to Pharmac, which was accepted, which allowed it to compete on an equal footing with Losec for a share of the PPI market.

Astra sued Pharmac. Among other things, it claimed damages for breaches by Pharmac of the confidentiality obligations in the Losec agreement. Astra's complaints concerned the provision of forecasts of expenditure by Pharmac to P&U which were said to disclose Astra's confidential information and the disclosure to P&U of the Losec agreement and in particular the clause dealing with the application of reference pricing. Astra did not succeed in the High Court but succeeded in part in the Court of Appeal. On the issues of confidentiality, the Court of Appeal held that:

- Pharmac was in breach of its obligations under the confidentiality clause in disclosing certain market forecast and share data of Astra, and in disclosing, without first reasonably informing Astra, the provisions for exemption from reference pricing of Losec in the Losec Agreement.
- Had Pharmac not breached its confidentiality obligations, an agreement to lift restrictions on Somac would have come into effect four months later than it did. This part of the judgment contains a useful discussion of loss of chance principles and the Court's approach to Astra's argument that, had it been properly informed of the proposed disclosure, it would have sought injunctive relief.[6]
- Astra was entitled to be compensated for the breaches on the basis that Pharmac had an improper headstart in entering the Somac derestriction agreement which, when it came into effect, reduced the subsidy payable from public funds to Losec.
- Because Astra had not established that it had incurred loss due to the reduction in subsidy, damages were to be assessed in terms of the opportunity cost to Astra of the reduction.

One of Pharmac's points of cross-appeal was that there had been no actionable breach of the confidentiality clause because Pharmac was protected against such a claim by section 48 of the Official Information Act. Section 48 provides that no proceedings shall lie in respect of the making available of official information in good faith, or for any consequences that follow from making it available. The Court did not agree that this clause protected Pharmac. It said Astra's claim did not arise from making available official information or consequences that followed from that. Rather, it arose from a failure to notify Astra in advance that the information would be made available, to which section 48 was not relevant.

Earlier in its judgment, the Court had commented on the confidentiality clause in these terms:[7]

> "… the obligation is expressed as prohibiting disclosure of confidential information other than, first, in accordance with a process (in essence requiring prior notice of intention to disclosure) and, secondly, in stipulated circumstances (in particular where a legal duty to make disclosure arises under the Official Information Act). The purpose of the obligation to reasonably inform the other party of an intention to disclose confidential information is, in our view, to allow the other party a reasonable period of time in which to consider its position, and take such steps as are open to it. These might be to make submissions to Pharmac (which however has public responsibilities under the Official Information Act which might require disclosure) or to seek redress, including injunctive relief, in the Courts. The clause requires that the other party be given sufficient notice of when information will be released to have a genuine opportunity to take such action prior to release. Properly understood it is not in conflict with the provisions of the Official Information Act".

## Comment

In the author's view, this logic is directly applicable to contractual consultation obligations requiring a U.K. public authority to consult an originator of information before disclosing it under FOIA. Provided they are drafted so as not to interfere with the temporal requirements of FOIA (*e.g.*, the expected time limit for complying with requests), they would not be inconsistent with the terms of FOIA and therefore not invalid on the ground of inconsistency with statute. Further, section 56 of FOIA would not protect the public authority. That section states that the Act does not confer any right of action in civil proceedings in respect of any failure to comply with any duty imposed by or under the Act. The section is silent on causes of action arising in contract. It is virtually inconceivable that a court would construe the provision in a way which excludes such causes of action.

The significance, for companies and public authorities alike, is that the breach of such a clause would in principle entitle the company to claim, from the public authority, damages arising

from the breach. In some cases those damages may be minimal. In others, like the Astra case above, they could be significant and give the company a measure of commercial leverage which it might otherwise not have had.

Although an earlier version of the FOIA Code discouraged public authorities from accepting confidentiality clauses, the kind of clause outlined above is not a true confidentiality clause; it simply stipulates a contractually permissible consultation procedure and recognises that disclosure may subsequently be required by law. In any event, some transactions may simply not go ahead if a public authority refuses to include such a clause.

## Conclusion

In the author's view, the conclusion is clear: a public authority which fails to comply with a properly drafted contractual obligation requiring consultation or notification prior to disclosure under the Act will not be able to argue successfully that the Act somehow immunises it from liability for breach. To the contrary, it will expose itself to a claim for damages for the harm suffered by its contractual counterparty as a result of the breach.

1 Available online at *www.dca.gov.uk/foi/codesprac.htm*

2 See paragraphs 25-30 of the Code.

3 One might argue, however, that at least a measure of statutory prescription is found in section 45(2)(c) of FOIA which states that the Code of Practice must include provisions relating to "consultation with persons to whom the information requested relates or persons whose interests are likely to be affected by the disclosure of information".

4 One might argue, for example, that the nature of the interests to be affected by disclosure are such as to warrant consultation as a matter of procedural fairness, that a legitimate expectation of consultation springs from the Code of Practice itself or past practice, or, at least, that *whether* to consult is a mandatory relevant consideration.

5 [2000] NZCA 345 (available online in full text via *www.worldlii.org/nz/cases/NZCA/*).

6 Those who may find themselves advising companies in the position of Astra may wish to read paragraphs 68 to 73 of the judgment.

7 Paragraph 37 of the judgment.

# Case Report

## GERMANY

### Selective E-Mail Filtering is Criminal Offence

#### *Case ref: I Ws 152/04,*

*Regional High Court of Karlsruhe , January 10, 2005*

Karlsruhe's regional high court has ruled that public bodies that filter former employees' e-mails may be guilty of a criminal offence.

The case was brought by a scientist against a university that had previously employed him. He had sent e-mails to, and received e-mails from, university employees through their university e-mail accounts. The university had forbidden him from using its e-mail server and applied a technical filter preventing him using it.

The court found that this selective filtering of individual e-mails infringed section 206 of the German criminal code (Strafgesetzbuch), which protects the integrity of e-mails within companies. Although the university was not a company, the court stated that section 206 applies to public bodies if their e-mail servers are used for non-official purposes; as was the case here.

However, the court said that filtering may be legal if it is necessary to prevent virus attacks or other damage to an e-mail system. It sent the case back to the lower court to clarify whether there had been any such risk here.

This is a potentially worrying precedent for any public body that filters its employees' e-mails. Unless it can show that its e-mail system is used only for official purposes, or that filtering is necessary to prevent damage to the system, its management personnel may attract criminal liability.

*By Julia Meuser, Freshfields Bruckhaus Deringer, Hamburg; e-mail: julia.meuser@freshfields.com*

# News

## FRANCE

### Opt-out Becomes the Rule for B2B Marketing

During its February 17, 2005 session, the French data protection authority (CNIL) reversed its position on e-mail direct marketing in the B2B context: the CNIL stated that the sending of a commercial message to an individual's professional e-mail account and for professional purposes is no longer subject to the individual's prior consent. Until then, the CNIL had favoured a strict interpretation of the law, considering that the opt-in requirement applicable to e-mail marketing also applied to individuals acting in their professional capacity. However, since the purpose of the opt-in rule is to protect consumers, not to adversely affect exchanges between businesses, it decided that opt-out should become the rule in the B2B context.

For further information (in French only), consult the CNIL website at: *www.cnil.fr/index.php?id=1780&news[uid]=238&cHash=6dd2646505.*

*By Christopher Kuner, a Partner with Hunton & Williams, Brussels; ckuner@hunton.com*

## GERMANY

### Federal Commissioner Issues Guidance on Internet Use in the Workplace

On March 8, 2005, the German federal data protection commissioner, Peter Schaar, who is also Chairman of the Article 29 Working Party, published a flyer on employee use of the Internet in the workplace. The principles are applicable both in the private and public sector. The Guidelines can be downloaded free of charge from the Internet (in German only) at: *www.bfd.bund.de/information/flyer_net.pdf*.

*By Christopher Kuner, a Partner with Hunton & Williams, Brussels; ckuner@hunton.com*

  WDPR ISSN 1473-3579

# Personal Data

## New Regulations Regarding the Processing of Personal Data in Italy: Part 1

*By Avv. Alessandro del Ninno, Information & Communication Technology Department, Studio Legale Tonucci, Rome. The author may be contacted at adelninno@tonucci.it.*

The first few months of 2005 marked the entry into force of several important acts enacted by the Italian Data protection Authority implementing and improving Italian Data Protection law, as set forth in the Italian Code on Privacy (legislative decree of June 30, 2003 no. 196). The Code entered into force on January 1, 2004 and replaced the previous Italian privacy law no. 675/1996.

In particular, at least five acts must be mentioned and analysed with regard to the important set of specific guarantees therein provided regarding the processing of personal data:

- the Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments (in force from January 1, 2005);
- the General Act of February 24, 2005 on the so-called "fidelity cards", enacted by the Italian Data Protection Authority ("IDPA");
- the general rules for the protection of privacy regarding the use of third generation video mobile phones, enacted by the IDPA on January 23, 2005.
- the general rules for the protection of privacy regarding the use of Radio Frequency Identification technolgies (RFID) with particular regard to "labels" inserted in products or in microchips, enacted by the IDPA on March 9, 2005;
- the general rules for the protection of privacy within the subscription of cable and digital TV services, enacted by the IDPA on March 7, 2005;

Part I of this article will discuss the Code of conduct and professional practice (as listed above). Part II of the article, to be published in the May issue of *World Data Protection Report*, will provide specific analysis of the other four acts enacted by the IDPA.

### Code of Conduct Relating to Consumer Credit

Article 12 of the Code on Privacy provides that the IDPA encourages, within the framework of the categories concerned and in conformity with the principle of representation, the drawing up of codes of conduct and professional practice for specific sectors, verifies their compliance with laws and regulations by also taking account of the considerations made by the entities concerned, and contributes to the adoption of and compliance with such codes.

Compliance with the provisions included in the codes of conduct and professional practice is a prerequisite for the lawful processing of personal data by public and private entities.

To date, five codes of conduct for processing personal data in specific sectors and for specific purposes (journalistic purposes, statistical and scientific purposes in the public sector, statistical and scientific purposes in the private sector, historical purposes, and – the latest – the applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments) have entered into force and have been appended to the Code on Privacy. In the coming months, six further codes of conduct for specific sectors will be enacted.

As of January 1, 2005, the processing of personal data within the framework of information systems controlled by private entities that are used for the purposes of consumer credit and/or concern reliability and timeliness of payments must be carried out in such a manner as to respect data subjects' rights, fundamental freedoms, and dignity, with particular regard to the right to personal data protection, confidentiality, and personal identity. The new code of conduct (which does not apply to the information systems controlled by public bodies, in particular it does not apply to the centralised risk service managed by the Italian Central Bank) in fact sets forth adequate safeguards and processing mechanisms to protect data subjects' rights. Such measures are also intended to limit the risks in accessing consumer credit details and reduce the risk of data subjects becoming heavily indebted.

### Main Definitions

The main definition contained in the code of conduct can be listed as follows:

- "credit application/relationship" shall mean any application or relationship concerning the granting of credit in the exercise of commercial and/or professional activities, in the form of a payment extension, a loan, or any other similar financial support as per the Consolidated Statute on Banking and Credit (legislative decree no. 385 of September 1, 1993);
- "remedying of defaults" shall mean to extinguish the defaults on money obligations due either to defaults on payments or payment delays without losses and/or balance receivables also in the form of interests and charges, as well as to extinguish said obligations by means other than the relevant performance, in particular following settlement and/or composition;
- "credit information system" shall mean any database concerning credit applications/relationships that is managed in a centralised fashion by a legal person, an organisation, an association and/or another private body

and can only be accessed by the entities communicating the information recorded therein and participating in the relevant information system. The system may contain, in particular,

negative credit information, only concerning credit relationships affected by defaults;

positive and negative credit information concerning credit applications/relationships irrespective of the existence of defaults as recorded in the system at the time they occurred;

- "manager" shall mean any private entity acting as controller of the processing of the personal data recorded in a credit information system and managing said system by setting out the mechanisms applying to its operation and use;
- "participant" shall mean any private entity that acts as a controller of the processing of the personal data that are collected in connection with credit applications/relationships, participates in the relevant credit information system based on an agreement and/or contract with the manager, and can use the data contained in the system, being under the obligation to notify the manager systematically of said personal data as related to credit applications/relationships within the framework of mutual data exchanges with other participants. Except for the entities providing credit-factoring services, a participant may be:
  - – a bank;
  - – a financial broker;
  - – any other private entity that, in the exercise of commercial and/or professional activities, grants an extension for the payment related to the supply of goods and/or services.
- "consumer" shall mean a natural person who, in connection with a credit application/relationship, acts for purposes that cannot be related to his/her professional and/or business activity, if any;
- "data retention period" shall mean the period during which the personal data related to credit applications/relationships are retained in a credit information system and can be used by participants for the purposes referred to in this code;
- "automated credit scoring techniques and/or systems" shall mean the mechanisms to organise, aggregate, compare and/or process personal data related to credit applications/relationships as consisting in the use of automated systems based on statistical methods or models with a view to assessing credit risk, whose results are expressed in the form of summary judgments, figures and/or a score that is/are associated with a given data subject and aim at providing the predictive and/or probability-based description of said data subject's risk profile, reliability and/or timeliness of payment.

### Purposes of the Processing and Data Processing Allowed

The personal data contained in a credit information system may only be processed by the manager and participants for the purpose of protecting credit and limiting the relevant risks, and in particular, to assess data subjects' financial status and creditworthiness or anyhow their reliability and timeliness of payment.

It is important to point out that no other purposes may be pursued, especially in connection with market surveys and/or the promotion, advertising and/or direct selling of products or services (which in the past have been the more frequent cases of further and illicit use of the related data).

A participant may access a credit information system also by consulting a copy of the respective database with regard to data that fall justifiably within its scope of interest and may only concern:

a. consumers that apply for and/or are parties to a credit relationship with said participant as well as any surety, including joint sureties,

b. entities acting in the context of their business and/or professional activities, in respect of which investigations have been started in order to set up a credit relationship or undertake a credit risk, as well as entities that are already parties to a credit relationship with said participant,

c. entities that are legally related to those referred to in letter (b) above, in particular because they act as joint sureties or else belong to corporate groups, providing the personal data to be accessed by the participant are factually necessary in order to assess financial status and creditworthiness of the entities referred to in said letter (b).

A credit information system may be accessed by a participant and/or a manager exclusively via a limited number of data processors and persons in charge of the processing, to be specified in writing, as well as by having regard only to such data as are absolutely necessary, relevant and not excessive in connection with the specific requirements resulting either from the investigations performed following a credit application or from the management of a credit relationship, which must be verifiable in concrete on the basis of the information available to said participant(s). The system may also be accessed by banks and financial brokers that are members of the participant's banking group in compliance with the aforementioned limitations and mechanisms, exclusively with a view to dealing with the investigations required either to set up a credit relationship with the relevant data subject or anyhow to undertake the relevant risk.

Participants shall access the credit information system via the mechanisms and tools, including electronic tools, that have been set out in writing jointly with the manager in compliance with personal data protection legislation. The personal data related to credit applications/relationships recorded in a credit information system may be consulted via stepwise, selective access mechanisms that shall envisage one or more consultation levels providing summary and/or condensed information in respect of the data subject prior to allowing access to detailed information, which shall also apply to the data concerning sureties and/or related entities. It shall not be feasible, also from a technical standpoint, to access the data in a manner allowing bulk queries and/or acquisition of lists of data regarding credit applications/relationships in respect of entities other than those applying for and/or participating in a credit relationship with the relevant participant.

Furthermore, third parties will not be permitted to access a credit information system except for the requests made by judicial and police authorities for purposes of justice, or else by other public institutions, authorities, administrative agencies and bodies exclusively in the cases referred to in laws, regulations and/or

 

Community legislation as well as in compliance with the relevant provisions.

Where the personal data contained in a credit information system are also processed by means of automated credit scoring techniques and systems, the manager and participants shall be responsible for ensuring compliance with the following principles:

- the techniques or systems made available by the manager, or else implemented on the participants' behalf, may only be used for investigating a credit application and/or managing the credit relationships already set up;
- the data concerning judgments, markers and/or scoring associated with a given data subject shall be processed and communicated by the manager only to the participant that either has received the relevant credit application from the data subject or previously communicated data related to the relevant credit application; at all events, the data may not be retained in the credit information system, nor may they be made available to the other participants;
- statistical models and/or factors as well as the algorithm used to calculate judgments, markers and/or scoring shall be verified regularly at least on an annual basis and updated as a function of the outcome of said verification;
- where a credit application is not granted, the participant shall inform the data subject as to whether it has consulted data related to negative judgments, markers and/or scoring that have been obtained by means of automated credit scoring techniques and systems, in order to investigate said credit application; if the data subject so requests, the participant shall provide him or her with the data in question and explain both the logic underlying operation of the systems implemented and the main factors that have been taken into account in processing the application.

## Categories of Data which can be Processed

Processing within the framework of a credit information system may only concern data related to the entity that either applies for or is a party to a credit relationship with a participant as well as the data related to any surety, including a joint surety, whose position is clearly separate from that of the principal debtor.

Processing may not concern sensitive or judicial data, and shall concern objective personal data that are closely relevant and not excessive in respect of the purposes sought and relate to a credit application/relationship as well as to any event occurring on whatever ground and for whatever purpose until remedying of the relevant defaults in compliance with the allowed retention periods.

Manager and participants shall take suitable technical, logical, informational, procedural, physical, and organisational measures to ensure security, integrity, and confidentiality of personal data and electronic communications in line with personal data protection legislation.

The manager shall take adequate security measures to ensure proper functioning of the credit information system as well as access control. Accesses shall be recorded and stored in the information system by the manager as well as by all participants in the possession of a copy of the relevant database.

As for compliance with the security, confidentiality, and secrecy obligations referred, manager and participants shall issue specific instructions in writing to the respective data processors and persons in charge of the processing and shall ensure that said instructions are fully abided by also by means of verifications carried out by suitable supervisory bodies.

## Communication of Data within a Credit Information System

The data related to the first payment delay in a credit relationship shall be used and made available to other participants in compliance with the terms below:

- in negative credit information systems, after at least 120 days as of the relevant payment deadline, or in case the debtor defaulted on at least four monthly instalments and these were not remedied;
- in positive and negative credit information systems,
  - – if the data subject is a consumer, after 60 days of the monthly update, or in case he/she defaulted on at least two consecutive monthly instalments, or if the delay has to do with either the last or the last but one instalment. In the second case referred to above, the data shall be made available after the monthly update concerning the second consecutive default;
  - – in all other cases, after at least 30 days following the monthly update, or in case the debtor defaults on one instalment.

In case of payment delays, the participant shall inform the data subject, also at the time reminders or other notices are sent, that his/her data will be shortly recorded in one or more credit information systems. The data concerning the first delay may be made available to participants after at least 15 days as of sending the aforementioned information to the data subject.

The data recorded in a credit information system shall be updated regularly at monthly intervals by the participant that has communicated them.

## Notifying the Data Subject

At the time of collecting the personal data related to credit applications/relationships, a participant shall inform the data subject pursuant to section 13 of the Code on Privacy also with regard to the processing of personal data that is performed within the framework of a credit information system.

The information shall include clear-cut, accurate details concerning, within the framework of the description of the purposes and mechanisms of the processing, by specifying the following:

- identification data concerning both the credit information systems and the personal data that are communicated to the respective managers;
- the categories of participant accessing said systems;
- the data retention periods in the credit information systems such data are communicated to;
- arrangements applying to organisation, comparison and processing of the data and the use, if any, of automated credit scoring techniques and/or systems;
- mechanisms for data subjects to exercise the rights referred to in section 7 of the Code on Privacy.

The IDPA has enacted a standard model which can be used by the operators as the information notice specifically related to credit information systems.

### Data Retention and Updating

This is the most important part of the Code of Conduct, since it introduces for the first time, clear rules relating to the maximum retention periods of the related personal data within a credit information system.

The personal data related to credit applications as communicated by participants may be retained in a credit information system for as long as necessary in order to deal with said applications and at all events for no longer than 180 days as of the date of submission of the aforementioned applications. If the credit application is not granted, or if it is waived, the participant shall inform the manager thereof in connection with the monthly update of the system. In the latter case, the personal data related to the application that has been waived by the data subject and/or rejected may be retained in the system for no longer than 30 days as of their update.

Negative credit information related to payment delays that are subsequently remedied may be retained in a credit information system:

- for up to 12 months as of the recording of the data concerning remedying of delays not in excess of two instalments/two months; or
- for up to 24 months as of the recording of the data concerning remedying of delays in excess of two instalments/two months.

Upon expiry of the terms referred to above, the data shall be removed from the credit information system if no data concerning further delays and/or defaults is recorded during said terms.

Participant and manager shall promptly update the data concerning remedying of defaults of which they are aware, where such remedying takes place after the participant's assignment of its credit to an entity that does not participate in the relevant system, also if the data subject so requests by submitting either a statement rendered by the credit assignee or any other suitable instrument.

Negative credit information related to defaults that are not subsequently remedied may be retained in a credit information system for no longer than 36 months as of the expiry of the relevant contractual agreement; if other events occur that are material to the payment, said information may be retained for no longer than 36 months as of the date on which the information had last to be updated or the relevant relationship was terminated.

Positive credit information related to a relationship that was concluded by extinguishing all monetary obligations may be retained in a system for no longer than 24 months as of the date of termination and/or expiry of the relevant contractual agreement, or else as of the first update performed in the month following the aforementioned dates. In light of the requirement whereby the data should be complete in respect of the purposes to be achieved, the aforementioned positive credit information may be retained further in the system if the latter contains negative credit information related to delays and/or defaults that have not been remedied with regard to other credit relationships concerning the same data subject. In the latter case, the positive credit information shall be removed from the system upon expiry of the term related to the retention of the negative information recorded in the system in respect of any other credit relationships concerning said data subject.

If the consumer concerned notifies a participant that he/she is withdrawing his/her consent to the processing of positive information within the framework of a credit information system, the participant shall inform the manager thereof in connection with the monthly update of the system. In the latter case as well as in case withdrawal of consent is communicated directly by a data subject, the manager shall record this news in the system and remove the information no later than 90 days as of said update and/or communication.

Prior to removing the data from a credit information system in accordance with the specifications set out in the above paragraphs, a manager may transfer the data to another medium in order to retain them exclusively for as long as necessary with a view to defending a legal claim, or else in order to process the data in anonymous format for statistical purposes.

### Access and Exercise of Other Rights by Data Subjects

With regard to the personal data recorded in a credit information system, data subjects shall be entitled to exercise their rights in accordance with the mechanisms set out in the Code on Privacy (see articles 7-10) both in respect of the manager and in respect of the participants that have communicated said data. The latter entities shall be responsible for dealing promptly and in full with the relevant requests, also by taking suitable organisational and technical measures.

In the request made to exercise his/her rights, a data subject shall also specify, if possible, his/her taxation ID and/or VAT Register number in order to facilitate searching the data concerning him/her in the credit information system.

Where it is necessary to carry out additional and/or specific controls with the participant, the manager shall inform the data subject thereof within a 15-day term and set another term for the relevant answer, which may not be in excess of 15 additional days. During the period required to carry out the additional controls with the participant, the manager:

- shall keep track of the performance of the aforementioned controls in the credit information system throughout the initial 15-day term, by means of a specific code and/or an ad-hoc message to be posted with the data that are the subject of the request made by the data subject, and
- shall suspend display of the data that are being controlled in the credit information system throughout the additional fifteen-day term.

### Sanctions

Without prejudice to such sanctions as are provided for by the administrative, civil, and criminal laws in force, managers and participants shall be subject to suitable mechanisms to impose sanctions that are proportionate to the seriousness of the relevant breaches. Such sanctions shall include an official warning, suspension or withdrawal of the authorisation to access the credit information system, and – in the most serious cases – publication of the news concerning the breach(es) in one or more dailies or magazines with nationwide circulation at the offender's expense.

 

# Canada: Transfers of Personal Information to U.S. "Linked" Service Providers

*By Andrea Freund, a Partner with Blake, Cassels & Graydon LLP, Toronto. The author may be contacted at andrea.freund@blakes.com*

Much attention has been focused recently in Canada on the privacy issues arising out of the use of service providers for data processing services where the data is either stored in the United States by a U.S. organisation or is stored in Canada by a Canadian organisation where such organisation has a U.S. affiliate (in each case, a U.S. linked service provider). This issue was highlighted with the release, on October 29, 2004, of the report of the Information & Privacy Commissioner for British Columbia entitled "Privacy and the USA Patriot Act" (the B.C. Report), which draws attention to the potential risks of using U.S. linked service providers to provide data processing or storage services. Furthermore, recent amendments to the British Columbia Freedom of Information and Protection of Privacy Act (FOIPPA) (which amendments came into force on receiving Royal Assent on October 21, 2004) were implemented at least in part to address concerns with outsourcing public body data processing activities to U.S. linked service providers.

The B.C. Report considers the implications of transfers of personal information for processing, particularly in light of the USA Patriot Act which, among other things, amended the U.S. Foreign Intelligence Surveillance Act (FISA) to permit U.S. authorities to obtain records and other "tangible things" as a way of protecting against international terrorism and clandestine intelligence activities. The USA Patriot Act also expanded the circumstances under which the FBI can issue national security letters in the United States to compel financial institutions, phone companies and Internet service providers to secretly disclose information about their customers. The B.C. Report underscores the concern that the Foreign Intelligence Surveillance Court could, under FISA (as amended by the USA Patriot Act), order a U.S.-located corporation to produce records held in Canada that are under the U.S. corporation's control. The B.C. Report indicates that some U.S. courts have found that, under U.S. law, control of records exists whenever there is a U.S. parent-Canadian subsidiary corporate relationship, regardless of the contractual or practical arrangements between the customer providing the data and the service provider or its U.S. parent; although the B.C. Report goes on to say that other U.S. cases suggest that contractual or practical arrangements may influence a U.S. court's findings regarding control. The report concludes that there is a reasonable possibility of unauthorised disclosure of British Columbians' personal information pursuant to an extra-territorial U.S. order or national security letter.

The B.C. Report underscores two possible privacy problems facing Canadian organisations in respect of their compliance with Part 1 of the Personal Information Protection and Electronic Documents Act (PIPEDA). The first potential problem arises in connection with the transfer of personal information for processing by a Canadian organisation to a U.S. linked service provider; the second stems from the possible disclosure of such information by the U.S. linked service provider pursuant to a U.S. court order. Similar issues may also apply to transfers of information for processing to organisations in jurisdictions other than the United States, but given the recent attention to the USA Patriot Act and its implications on privacy rights, this article focuses in particular on the provision of personal information to organisations located in, or connected to, the United States.

## Transfer of Personal Information by Organisation to U.S. Linked Service Provider

Section 4.1.3 of Schedule 1 to PIPEDA provides that,

> "[a]n organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing" and that it "shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party".

It is questionable whether, in light of the fact that disclosure of personal information could be required under U.S. law, it is possible for an organisation transferring information to a U.S. linked service provider, to provide a comparable level of protection, regardless of whether it requires the receiving organisation, in a contract or otherwise, to do so. It could be argued that a risk of a U.S. linked service provider being ordered to disclose the information to U.S. authorities is not a risk that is unique to U.S. linked service providers since information held by organisations in Canada may also be subject to orders for disclosure to Canadian or foreign authorities (for example, pursuant to the Canadian Securities Intelligence Service Act or tax and other treaties). The risk of possible ordered disclosure in the United States, therefore, would not seem to render a U.S. linked service provider less capable than an organisation in Canada of providing comparable protection since risks of ordered disclosure exist in respect of organisations in Canada as well. It is essential, though, that steps be taken, such as the entering into of a data protection agreement with the service provider, to ensure that the service provider implements measures to protect the security of the personal information.

Consideration should also be given to informing the individuals whose information is being transferred about the risks of disclosure of the personal information by the U.S. linked service provider and whether obtaining the individual's consent to such transfer in that case is reasonable, or whether it could offend section 4.3.3 of Schedule 1 of PIPEDA. Such section provides that,

> "[a]n organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes".

The analysis of what is required to fulfil the purposes will depend on the particular facts and circumstances.

## Disclosure of Personal Information by a U.S. Linked Service Provider Pursuant to a U.S. Court Order

The exceptions in PIPEDA permitting disclosure without consent refer broadly to laws and orders without expressly stipulating whether the references include foreign laws and orders or are to be restricted to domestic laws and orders.

Disclosure without consent is permitted in specified circumstances, including where disclosure is:

- required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records (section 7(3)(c));
- made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law (section 7(3)(c.1)(ii)); and
- required by law (section 7(3)(i)).

Although PIPEDA does not expressly require that the court, person or body with jurisdiction, the government institution or the law, as referred to in the sections of PIPEDA mentioned above, need be Canadian, a court could conceivably narrowly interpret the legislation. It is interesting in that regard that the B.C. Privacy Commissioner concluded in the B.C. Report that disclosure of personal information in response to a foreign law or order is "unauthorized" for the purpose of section 30 of FOIPPA, which section places an obligation on a public body to make reasonable security arrangements against such risks as unauthorized disclosure, because "a foreign law does not apply in British Columbia".

Also, the federal Privacy Commissioner, in her submission to the Office of the Information and Privacy Commissioner for British Columbia, expressed her view that any order made by a foreign government or court would have no legal force against a company, based only in Canada, that maintains personal information only in Canada. She did, however, state that organisations operating in a foreign country that hold personal information about Canadians in that country must comply with the laws of that country such that if they are presented with an order requiring them to disclose personal information, they must surrender that information. Of note, the Alberta private sector privacy legislation also has an exception permitting disclosure without consent where the disclosure is pursuant to statute or regulation that authorises or requires the disclosure but such exception is restricted to statutes or regulations of Alberta or Canada.

PIPEDA is scheduled for legislative review in 2006. Given the concerns about cross-border exchanges of information, it is hoped that amendments to PIPEDA that specifically address these concerns will be introduced in conjunction with, or following, such review. In the meantime, though, organisations will continue to grapple with how best to structure outsourcing or other arrangements involving the transfers or disclosures of personal information outside of Canada.

# Security & Surveillance

## The Coming Expansion of Corporate Information Security Obligations

*By Thomas J. Smedinghoff, a Partner with Baker & McKenzie and North American Co-ordinator of the Firm's Electronic Commerce Law Practice. The author is based in the Chicago office of Baker & McKenzie and may be contacted at smedinghoff@bakernet.*

A series of recent events are likely to lead to a significant expansion of corporate obligations to provide security for digital information. New legislation, regulations, and lawsuits all focused on the adequacy of corporate security have quickly followed several well publicised security breaches. As a result, companies need to look closely at the state of their compliance efforts in this highly charged environment.

Several recent security breaches involving the loss or disclosure of personal information held by information brokers, major banks, universities, and others are generating strong pressures for enhanced corporate legal obligations to implement appropriate information security measures to protect personal data. And corporate obligations to protect other data will likely be caught up in the process as well.

The legal response to recent events has focused primarily on corporate obligations to:

- provide adequate security for corporate information;
- implement appropriate internal incident response procedures;
- disclose breaches involving personal information to those affected.

The net effect is likely to be the imposition of new and significant legal obligations on most businesses, as well as increased enforcement of existing obligations.

### The Genesis of the Current Controversy

Described by many as the "perfect storm," the current controversy began with a disclosure by ChoicePoint, a company previously unknown to most people, that personal information it had collected on 145,000 individuals had been compromised, and was at risk of unauthorised use for purposes such as identity theft. ChoicePoint collects information on most U.S. households and their inhabitants, and is a leading provider of identification and credential verification services to business, government and individual customers. Apparently criminals posing as legitimate small business operators signed up as customers of ChoicePoint and acquired the personal records via normal customer channels.

That news was quickly followed by several other cases of apparent security breaches. First, a major bank disclosed that backup tapes containing credit card records on approximately one million individuals, including several U.S. Senators, were missing after being sent to an off-site storage facility. Then a second information broker revealed that hackers commandeered one of its databases, gaining access to the personal files of as many as 32,000 people. Thereafter, disclosures by two universities that hackers had broken into their computers and may have obtained access to personal information on up to 120,000 alumni (at a private college) and up to 59,000 current, former, and prospective students, faculty, and staff (at a public university) further fueled the controversy.

The immediate reaction has led to a legislative and regulatory fury. Several bills focused on corporate information security obligations have been introduced in Congress, financial industry regulations to address this issue have been finalised, and over 60 bills have been introduced in at least 36 states. In addition, Congress has been holding hearings on the issue of information security, particularly as it relates to personal information.

### The Coming Expansion of Security Law

The emerging trend is quite clear, and the implications for most companies will be significant. We are witnessing a ground swell of support for the notion that the security of corporate information is a major concern for all corporate stakeholders, and there is increasing recognition that taking appropriate steps to ensure the security of that information is (or should be) a legal obligation. Thus, when the dust settles, we are likely to see major changes in two areas. The first is significant expansion of corporate information security obligations. The second is a move from industry-specific and data-specific regulation to a broad application of information security obligations to all industries and all types of important data.

Historically, corporate legal obligations to implement security measures have been set forth in a patchwork of federal and state laws, regulations, and government enforcement actions, as well as common law fiduciary duties and other implied obligations to provide "reasonable care."[1] Most requirements have been industry-specific (*e.g.,* focused only on financial industry or the healthcare industry) and data-specific (*e.g.,* focused only on personal data). But that is changing.

In early 2003, the U.S. *National Strategy to Secure Cyberspace* argued for a much broader approach to corporate security. Noting that most business entities "have become fully dependent upon information technology and the information infrastructure",[2] the *National Strategy* sought to move the debate beyond specific industry sectors and specific types of data, asserting that "*all users* of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace."[3]

In March 2005 testimony before Congress, the Chairman of the Federal Trade Commission, Deborah Platt Majoras, provided further support for this view by suggesting that the

extensive scope of the security obligations imposed on the banking industry[4] should be expanded to cover all industries. And, in fact, this has essentially been FTC policy in its enforcement actions and resulting consent decrees.[5]

In addition, recently filed class action lawsuits brought against ChoicePoint also suggest efforts to broaden the scope of corporate security obligations, with a view to protecting the interests of major stakeholders. The first suit, brought on behalf of individuals whose personal data was compromised by the security breach, alleges that ChoicePoint failed to implement adequate security measures, and failed to timely and fully disclose the breaches once they occurred.[6] The second suit, brought on behalf of shareholders, alleges that ChoicePoint and its management failed to disclose to shareholders and potential investors that the company's security measures were inadequate and ineffective.[7]

## What Companies Need to Do Now

The law regarding corporate information security obligations has been steadily developing for some time now.[8] But the uproar caused by the ChoicePoint incident is clearly accelerating this process. The bottom line for most businesses is that prompt action on a legally compliant information security programme has now become crucial. Do not wait for more laws to be enacted. Compliance takes time, and given the current climate, even the public relations impact of a security breach can be problematic.

The occurrence of a security breach does not, by itself, establish that a company's security programme is inadequate or fails to comply with applicable legal standards. At the same time, however, the fact that a security breach has not yet occurred does not establish the sufficiency of a company's information security programme.[9] And with the intense pressure generated by the recent highly publicised events in the security area, we can expect increased scrutiny of corporate security programmes on a variety of fronts.

The key issues raised by the current events, the proposed legislation, and the Congressional hearings are as follows:

### Risk Assessment and Responsive Measures

Developing a legally compliant security programme is critical. Most recent statutes and security regulations in both the United States and Europe make this a priority.[10] While the legal standards for such a programme are still developing,[11] a key component is to implement a periodic risk assessment process.

This involves identifying all reasonably foreseeable internal and external threats to the information assets to be protected. Threats should be considered in each area of a company's operation, including information systems, network and software design, information processing, storage and disposal, prevention, detection, and response to attacks, intrusions, and other system failures, employee training and management. For each identified threat, the company should then evaluate its risk by:

- assessing the likelihood that the threat will materialise;
- evaluating the potential damage that will result if it materialises; and
- assessing the sufficiency of the policies, procedures, and safeguards in place to guard against the threat.

This process will be the baseline against which a security programme can be measured and validated. The goal is to understand the risks a business faces, and determine what level of risk is acceptable, in order to identify appropriate and cost-effective safeguards to combat that risk.

In other words, it is not enough merely to implement impressive-sounding security measures. They must be responsive to the particular threats a business faces, and must address its specific vulnerabilities. Posting armed guards around a building, for example, sounds impressive as a security measure, but if the primary threat the company faces is unauthorised remote access to its data via the Internet, that particular security measure is of little value. Likewise, firewalls and intrusion detection software are often effective ways to stop hackers and protect sensitive databases, but as the ChoicePoint case illustrates, if a company's major vulnerability is giving access to the wrong people, perhaps because they are not properly authenticated, then even those sophisticated technical security measures, while important, will not adequately address the problem.

### Incident Response Plan

How a company responds to security breaches when they occur is also a key issue. Prompt action on a variety of fronts is critical, both from a legal and a public relations perspective.

Thus, it is important to recognise that, as part of such a security programme, companies need a well thought out and legally compliant incident response plan. Such plan should ensure that appropriate persons within the organisation are promptly notified of security breaches, and that prompt action is taken both in terms of responding to the breach (*e.g.,* to stop further information compromised and to work with law enforcement), and in terms of notifying appropriate persons who may be potentially injured by the breach.

ChoicePoint was criticised in Congressional hearings, for example, because its September 27, 2004 discovery of a possible security breach was apparently not brought to the attention of senior management for approximately six weeks. Companies need incident response plans in place so that prompt action can be taken.

### Security Breach Notification

Perhaps the most significant legal obligation raised by the recent series of security breaches, however, is the duty to notify persons who may be affected by the breach (*e.g.,* persons whose personal information has been disclosed).

Recognition that the security of personal information stored in large commercial databases is beyond the control of the data subjects has given many cause for concern. Thus, as an initial response, much of the legislative and regulatory activity focuses on a company's obligation to disclose breaches of personal information to the individuals whose data has been compromised. This approach seeks to impose on companies an obligation similar to the common law "duty to warn" of dangers. Such a duty is often based on the view that a party who has a superior knowledge of a danger of injury or damage to another that is posed by a specific hazard must warn those who lack such knowledge.

The first law to adopt this approach for personal information was the California Security Breach Information Act (S.B. 1386), which became effective on July 1, 2003.[12] That law requires all

companies doing business in California to disclose any breach of security that results in an unauthorised person acquiring certain types of personally identifiable information about a California resident. Disclosure must be made to all persons whose personal information was compromised, and anyone who is injured by a company's failure to do so can sue to recover damages. Many credit this law for inducing companies to make the breach disclosures mentioned above.

The concept is not new, however. In 1998 the Internal Revenue Service imposed a disclosure requirement on taxpayers whose electronic records were the subject of a security breach. In a Revenue Procedure that sets forth its basic rules for maintaining tax-related records in electronic form, the IRS requires taxpayers to "promptly notify" the IRS District Director if any electronic records "are lost, stolen, destroyed, damaged, or otherwise no longer capable of being processed …, or are found to be incomplete or materially inaccurate."[13]

The most expansive security breach disclosure requirements to date appear in rules just adopted by several Federal financial regulatory agencies in March 2005.[14] These regulations require financial institutions to develop a response programme to protect against and address breaches of the security of customer information maintained by the financial institution or its service provider. Such programme must include procedures for notifying customers, as well as regulatory and law enforcement agencies, about incidents of unauthorised access to customer information that could result in substantial harm or inconvenience to the customer.

The next steps in this emerging trend may well take place in Congress. The "Notification of Risk to Personal Data Act"[15] has again been introduced by Senator Feinstein. Similar to the California Act, it would apply nationwide and require anyone that owns or licenses electronic data containing personal information to notify any person whose personal information was acquired by an unauthorised person through a breach of security. At present, some form of Feinstein's bill is given a good chance of passage.

The bottom line is that security breach notification obligations, at least with respect to the compromise of personal information, will very likely become law at the federal level and/or in most states sometime this year. And while the initial thrust of such laws will be to focus on notifying individuals if their personal information has been compromised, it is very likely that such obligations will ultimately expand to include disclosure to other stakeholders of security breaches that affect their interests as well. This may include, for example, disclosures to shareholders and investors of breaches involving financial information, disclosures to the IRS regarding breaches of tax-related information, and disclosures to other regulatory agencies that may have an interest in the impact of the security breach.

### Monitor Outsource Providers

Finally, businesses also need to recognise that the increased scrutiny of the legal compliance of their information security measures also extends to corporate information that is under the control of and processed by a third party outsource provider. Outsourcing work to a third party does not relieve a company of its obligations with respect to the security of the information outsourced. As a consequence, businesses will need to look not only at their own security measures, but also at the security measures of the outsourced providers with whom they contract.

## Conclusion

In the final analysis, in today's network environment, companies have an almost total reliance on digital information. Yet the form in which that information is created, used, communicated, and stored helps to facilitate certain types of compromise, often on a massive scale, and quick communication and utilisation of the compromised information for fraudulent purposes. Thus, there is no escaping the fact that information security is a critical issue – and one that is rapidly becoming a legal obligation.

As the recent rash of security incidents demonstrates, there are many different ways in which security breaches can occur. Although attacks by outside hackers are often seen as a primary concern, the recent cases clearly indicate that security breaches can be the result of inappropriate conduct by insiders with authorised access, a failure to properly authenticate third parties given access to the information, stolen laptops, and lost or stolen media containing sensitive information. But in all cases, one thing is clear. Regardless of how the security breach occurs, the storage of information in a digital form facilitates the ready compromise of massive amounts of sensitive information, in many cases with little effort, and in some cases without immediate detection.

In addition, the public relation consequences for companies can be significant. Most of the companies that have suffered security breaches are viewed as the culprits (for failure to implement appropriate security), rather than the victims of a crime by outsiders. In the past, when a bank was robbed at gunpoint, we chased the bank robber. Today, when a company is robbed digitally, the tendency seems to be to blame the company for its lack of security, and to call for new laws imposing new requirements to prevent the event from happening a second time.

1 For a compilation of some of the laws governing information security, see *www.bakermet.com/ecommerce*.

2 *National Strategy to Secure Cyberspace*, February 14, 2003, at pp. 5-6, available at *www.whitehouse.gov/pcipb*

3 *National Strategy* at p. 37 (emphasis added).

4 See, Gramm-Leach-Bliley Act ("GLBA"), Public Law 106-102, ss. 501 and 505(b), 15 U.S.C. ss. 6801, 6805, and implementing regulations at 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision) and 16 C.F.R. Part 314 (FTC).

5 See, *e.g., In the Matter of MTS, Inc., d/b/a Tower records/Books/Video* (FTC File No. 032-3209, April 21, 2004), available at *www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf*; *In the matter of Guess?, Inc*. (FTC File No. 022 3260, June 18, 2003), available at *www.ftc.gov/os/2003/06/guessagree.htm*; *FTC V. Microsoft*, Consent Decree (FTC, August 7, 2002); available at *www.ftc.gov/os/2002/08/microsoftagree.pdf*; and *In the Matter of Eli Lilly and Company*, Decision and Order (FTC Docket No. C-4047, May 8, 2002); available at *www.ftc.gov/os/2002/05/elililly do.htm*.

6 *Goldberg v. ChoicePoint*, Inc. No. BC329115, (Los Angeles Superior Ct., filed Feb. 18, 2005).

7 *Perry v. ChoicePoint, Inc*. No. CV-05-1644 (C.D. Cal., filed March 4, 2005).

8 See, *e.g.,* Thomas J. Smedinghoff, *Trends in the Law of Information Security*, *World Data Protection Report*, (August 2004).

9 See, Prepared Statement of the Federal Trade Commission before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, U.S. House of Representatives on "Protecting Our Nation's Cyberspace," April 21, 2004, at pp. 5-6, available at *www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf*.

10 In the U.S., see, *e.g.,* Gramm-Leach-Bliley Act ("GLBA"), Public Law 106-102, ss. 501 and 505(b), 15 U.S.C. ss. 6801, 6805 and implementing regulations at 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D-2.II(A) ("implement a comprehensive written information security program") (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision) and 16 C.F.R. Part 314.3(a) ("develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts") (FTC); Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. 1320d-2 and 1320d-4, and implementing regulations at 45 C.F.R. Part 164; Federal Information Security Management Act of 2002 ("FISMA"), 44 U.S.C. Section 3544(b) ("develop, document, and implement an agencywide information security program"); FTC Consent Decrees ("Establish and maintain a comprehensive information security program in writing"). In Europe, see, *e.g.,* Italy, Personal Data Protection Code, section 34(g) and Annex B, section 19; Spain, Law 15/1999 on the Protection of Personal Data, Article 9, and Royal Decree 994/1999; Netherlands, Personal Data Protection Act, Article 14(5).

11 See, *e.g.,* Thomas J. Smedinghoff, *The Developing U.S. Legal Standard for Information Security*, available at *www.bakerinfo.com/ecommerce/us%20cybersecurity%20standards.pdf*.

12 Cal. Civil Code section 1798.82. A copy is available at *www.leginfo.ca.gov/calaw.html*.

13 Rev. Proc. 98-25, section 8.01.

14 See "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice", Final Rule, jointly adopted by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and the Office of Thrift Supervision; available at *www.occ.treas.gov/consumer/Customernoticeguidance.pdf*.

15 See Senate Bill 115, introduced April 2005.

# News

## ITALY

### Data Protection Authority Issues RFID Guidelines

On March 29, 2005 the Garante (Italian Data Protection Authority) published guidelines on the processing of personal data by RFID chips. The Guidelines set forth the following general principles for use of the chips:

- individuals must be informed about their use;
- explicit consent must be given for the processing of personal data;
- there must be a way to deactivate the chips;
- labour law rights of employees must be respected;
- chips implanted under the skin may be used only in very exceptional cases;
- the principles of proportionality and finality must be observed and the personal data may be retained only as long as necessary;
- adequate security must be used; and
- the processing must be notified to the Garante.

The Guidelines are available (in Italian only) at: *www.garanteprivacy.it/garante/doc.jsp?ID=1109670.*

*By Christopher Kuner, a Partner with Hunton & Williams, Brussels; ckuner@hunton.com*

# 27TH INTERNATIONAL CONFERENCE ON PRIVACY AND PERSONAL DATA PROTECTION

**The 27th International Conference on Privacy and Personal Data Protection will be hosted by the Swiss Federal Data Protection Commissioner this year and will take place from September 14-16, 2005 in Montreux, Switzerland. Further information is available at *http://privacyconference2005.org*.**

## The Barbara Wellbery Memorial Award

The Barbara Wellbery Memorial Award, annual international privacy writing competition, was established in 2004 to honour the memory of Barbara Wellbery, a former partner at Morrison & Foerster, and her contribution to the privacy field. The purpose of the award is to spark constructive debate, stimulate creative thinking in the field of data privacy, and encourage the development of practical solutions to current privacy dilemmas. The first award was presented last year at the 26th Conference on Data Protection and Privacy Commissioners in Poland to Lilian Edwards from the Law Faculty of Edinburgh University in the U.K..

The award is granted annually by the Morrison & Foerster Foundation and submissions for the 2005 Award are now being accepted. The winner of the award receives a $3,000 cash award. In addition, the individual will receive an invitation to present his or her paper at an international data protection and privacy conference.

To view application information, the submission form and the 2004 winning entry, visit *http://mofo.com/news/media/files/pr02000.html*. For further information about award and guideline submissions, please contact Ms. Cynthia Rich of Morrison & Foerster LLP at crich@mofo.com.

 