Criminal provisions should be reviewed in the new UK Act

The criminal law amendments to the UK Data Protection Act include a number of apparent loopholes which need to be addressed in the new law, writes solicitor, Angus Hamilton.

The 1984 UK Data Protection Act was amended in February 1995 by the ragbag of criminal law alterations that constitute the Criminal Justice and Public Order Act 1994 (PL&B May '97 p.11, Feb '95 p.16). The amendments stemmed, not from any fundamental criticisms of the original statute, nor from proposals for streamlining from the Office of the Data Protection Registrar but, apocryphally, because someone played a practical joke on the new head of British Intelligence, Stella Rimington.

Ms Rimington was the first named head of British Intelligence, and the press decided to celebrate this limited openness by seeing what other confidential information could be unearthed about her. Investigative journalists therefore set about finding out details about her financial affairs by duping various data users (banks, utilities, etc.) into parting with her personal data. When a complaint was made to the Office of the Data Protection Registrar, it was decided that no prosecution could be brought since the duped data users had not committed any knowing or reckless breach of their register entry.

Amendments to curb private eyes

In truth, it is unlikely that this incident alone sparked the alterations to the Act - rather it was symptomatic of a general concern about the ease with which private detectives and journalists were apparently able to obtain purportedly confidential personal information. Some private investigators even boasted in advertisements that they could obtain "full financial profiles" of any individual.

The amendments (see box below) are fundamentally well-intentioned but, in reality, are not very well drafted, and consequently fraught with potential difficulties. Despite this, the current Government has signalled its intention to retain the provisions (albeit in an amended form) in the new Data Protection Act 1998, which will

Data Protection Act 1984 - Section 5 as Amended

5(1) A person shall not hold personal data unless an entry in respect of that person as a data user, or as a data user who also carries on a computer bureau, is for the time being, contained in the register.

5(2) A person in respect of whom such an entry is contained in the register shall not -

(a) hold personal data of any description other than that specified in the entry;

(b) hold any such data, or use any such data held by him, for any purpose other than the purpose or purposes described in the entry;

(c) obtain such data or information to be contained in such data, to be held by him from any source which is not described in the entry;

(d) disclose such data held by him to any person who is not described in the entry; or

(e) directly or indirectly transfer such data held by him to any country or territory outside the United Kingdom other than one named or described in the entry.

5(3) A servant or agent of a person to whom subsection (2) above applies shall, as respects personal data held by that person, be subject to the same restrictions to the use, disclosure or transfer of the data as those to which that person is subject under paragraphs (b), (d), and (e) of that subsection and, as respects personal data to be held by that person, to the same restrictions as those to which he is subject under paragraph (c) of that subsection.....

5(6) A person who procures the disclosure to him of personal data the disclosure of which to him is in contravention of subsection (2) or (3) above, knowing or having reason to believe that the disclosure constitutes such a contravention, shall be guilty of an offence.

5(7) A person who sells personal data shall be guilty of an offence if (in contravention of subsection (6) above), he has procured the disclosure of the data to him.

5(8) A person who offers to sell personal data shall be guilty of an offence if (in contravention of subsection (6) above), he has procured or subsequently procures the disclosure of the data to him.

implement the EU Directive by October 1998. (http://www.homeoffice.gov.uk/datap1.htm for details of the Government's proposals).

Exploiting a loophole in the law

Since subsections 7 and 8 are wholly dependent on a Section 5 (6) offence being committed, it is sensible to concentrate on the elements of that offence. The subsection suggests that an offence is only committed if the procurer obtains a disclosure *to himself*. This is in marked contrast to, for example, Section 16 of the Theft Act, which makes it an offence for a person by any deception to dishonestly obtain for *himself or another* any pecuniary advantage.

This might seem a minor point but it is an apparent loophole which appears ripe for exploitation. For example, a private detective agency procuring the disclosure of confidential financial information may be able to arrange for the data to be disclosed directly to their client, rather than to the original information procurer.

It might be argued that the client, by employing the agency, is also a "procurer", but the mental elements of the offence are going to be nearly impossible to establish in respect of a client. Such a person is probably going to be unaware of which data users the agency is going to approach, let alone the methods to be used to extract information. If the client knew all that, then they would hardly be paying an agent in the first place.

The problem is capable of quite simple resolution by the insertion of the words "or another" after the phrase "the disclosure to him" in the subsection. The implicit problems caused by this apparent oversight have already been made explicit in a prosecution brought by the Office of the Data Protection Registrar against a mortgage broker in February 1997.

Prosecution lost on technicality

The allegation, under Section 5(6) of the Act, that the broker had attempted to obtain a disclosure of personal financial information from a Credit Reference Agency, foundered on the fact that the arranged disclosure was not to the original procurer.

It is a requirement of the offence that the procurement results in a breach of Sections 5(2) or 5(3) of the Act - these are the provisions which oblige a data user to operate within the terms of the user's data protection register entry. Given that the emphasis in 5(6) is on procuring a disclosure, it might be presumed that the only possible relevant breach of 5(2) would be under subsection (d) which prohibits disclosures to a person not mentioned in a register entry. However, the wording of Section 5(6), possibly unintentionally, does not refer to 5(2)(d) alone but to the entirety of 5(2) which seems to admit the possibility of a 5(6) prosecution being founded on a consequential unauthorised use of personal data (5(2)(b) of the Act) or an unauthorised overseas transfer (5(2)(e)) and not just an unauthorised disclosure.

Establishing unauthorised disclosures

This is important because arguably it is going to be easier to establish an unauthorised *use* of personal data in a Section 5(6) scenario than an unauthorised *disclosure*. This is because data users (especially large-scale ones) are quite conservative in defining their actual or potential uses of data, but seem to adopt a very open-ended approach in defining classes of disclosures. Thus, a journalist deceiving a large utility into disclosing personal financial information may be able to argue that they are a "person making an enquiry" (a commonly chosen category of disclosures) but would have difficulty in squeezing the purpose of "investigative journalism" into, for example, one of British Gas's registered purposes.

The problem of data procurers claiming that they fall into a category of disclosures in the data user's register entry (and thus that no Section 5(2) breach has occurred) may also be countered by contending that if a procurer pretends to be one category of data user (a very common ploy with detective agencies and journalists) then they cannot claim the benefit of being, in reality, in another category. Thus, if a journalist obtains confidential financial information from British Gas by pretending to be a data subject, then they would be lumbered with the definition "person pretending to be a data user" (not a category to which any data user would register to disclose) and could not claim that they were also a "person making an enquiry" or any other category of disclosees.

The Office of the Data Protection Registrar has a number of forthcoming test prosecutions around

these issues, after which the law (or indeed the need to reform it) may become clearer.

"Reason to believe" difficult to interpret

Finally, problems arise with trying to establish the mental element in Section 5(6) offences. The subsection requires that the procurer knows or has reason to believe that a breach of 5(2) has resulted from their actions. In practice, knowledge is going to be extremely difficult to establish since it suggests a detailed knowledge of the duped data user's data protection register entry.

"Reason to believe" sounds like a familiar legal concept, but in reality it is a phrase that does not appear anywhere else in the criminal law. The legislators seem, almost wilfully, to have made a rod for their own backs by choosing a new phrase, rather than an equivalent concept such as "having reasonable grounds for suspecting" which does already exist (s.24 Police and Criminal Evidence Act 1984) and which has been the subject of judicial consideration and interpretation.

In practice, it is likely that the Data Protection Registrar will invite the courts to infer "reason to believe" whenever a deception has been practised by the procurer - on the basis that no deception would have been used if the procurer believed that they were acting within the terms of the data user's register entry.

Arguably, large-scale data users are unlikely to have to worry about Sections 5(6) - 5(8) of the Act very much, although the development of sharp practices and corner-cutting amongst staff should always be monitored. It is far more likely that they will be victims of such offences than the perpetrators.

However, even being a victim is undesirable since it carries the implication of lax security within the data user's organisation. It may also suggest a breach of the eighth Data Protection Principle, which requires data users to ensure that appropriate security measures are in place to prevent unauthorised access to or disclosure of personal data.

The reforms introduced by the Criminal Justice and Public Order Act were aimed at a clear evil, but it is questionable whether they hit their target. It may be that, despite the relative novelty of the new subsections, they are already ripe for review under the new Data Protection Act that will come into force before October 1998.

The author, Angus Hamilton, a solicitor, runs his own practice. Since 1986, he has conducted prosecutions under the Data Protection Act for the Office of the Data Protection Registrar and has advised corporations on data protection compliance and other matters relating to computing and the law. This year, he has spoken at our Roundtable in Edinburgh and at our Cambridge Conference. He is writing a new guide to data protection law.

Contact: Hamiltons, 42B, Independent Place, Shacklewell Lane, London, E8 2HE.
Tel: 0171 923 7823 Fax: 0171 249 2330
E-mail: Angus.Hamilton@btinternet.com.
Website http://www.btintemet.com/~hamiltons

Private Eye Guilty of Deceiving BT

At Harrow Magistrates' Court on October 28th 1997, Rachel Barry, a former private investigator, was convicted of a total of 12 offences of procuring the disclosure of personal data and of selling the information procured, in contravention of sections 5(6) and 5(7) of the Data Protection Act 1984.

Mrs Barry used deception to obtain information from BT (formerly known as British Telecom), such as ex-directory numbers and itemised bills, relating to people in whom the media were interested. Her clients included the proprietors of the mass circulation Sunday newspapers, *News of the World, The People, The Sunday Express* and *The Mail on Sunday*. She pleaded guilty to all 12 offences and was fined a total of £600 for the offences of procuring the information, and a total of £600 for selling the information. She was also ordered to pay costs of £800.

Commenting on the case the Data Protection Registrar (DPR), Elizabeth France, praised the co-operation BT had given her Office: "When the amendment was introduced, the concern and the intention of Parliament were clear, but we said then that convictions would only be secured with the co-operation of targeted data users. We are now working with a number of them to make clear that this kind of invasion of personal privacy is unacceptable." She added that in this case she was also particularly grateful for the co-operation of the witnesses who had suffered as a result of these offences. (Edited report from the Office of the DPR)