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)