UK Criminal Justice and Police Bill allows legal computer searches

Report by Susan Singleton

ON JANUARY 18TH 2001 the Criminal Justice and Police Bill received its first reading in the UK Parliament. Although designed mainly to increase police powers against offenders and help reduce crime and the fear of crime, the Act also contains important provisions about data protection.

Section 49 of the Bill allows police and customs officers to copy the hard drive of computer devices found during a legal search where there is a reasonable belief that the disk contains something relevant for which they are searching. Someone bringing a laptop computer that contains pornography from the US to the UK could be committing a serious arrestable offence and would be liable to a search as they enter the country.

THE CURRENT SITUATION

A second reading followed on January 29th and, in early May, the Bill entered the committee stage in the House of Lords. Whatever changes are made to the law in the future, at present customs officers do sometimes check computers of people entering the country. A quick check, often searching briefly for pornography, is likely. Customs and Excise have no current plans to make copies of contents of hard drives. A spokesperson said, "We will see what happens with the Police Bill. Currently we are simply allowed to check hard drives for pornography. Our current law does not entitle us, or the police, to seize material from one place in order to examine it elsewhere. But since we are looking for pornography, not product plans or personal banking information, normal people shouldn't worry." Worried business people might try to encrypt their systems to prevent company secrets being accessed. However, failure to hand over encryption keys would be an offence under the Regulation of Investigatory Powers Act 2000 (RIP). Failure to produce the relevant key could lead to a two year jail sentence.

BILL CLARIFIES LAWFUL APPLICATION OF NEW DNA TECHNOLOGY

The Home Secretary Jack Straw said that the Home Office hoped to increase the national DNA database from its current one million samples to 3.5 million in the next three years. DNA is one of the most private and personal forms of personal data available. It shows the predisposition of the data subject to various genetic disorders, gives their sex, establishes their paternity or otherwise to their children and can link them definitively to crimes.

Not surprisingly, therefore, data protection implications arise. The Bill amends parts of the Police and Criminal Evidence Act (PACE) dealing with the taking, storage and retrieval of fingerprints, footprints and DNA, to take account of developments in technology. It makes provision for electronic capture and storage of fingerprints. It provides for the taking of fingerprints and non-intimate samples without consent and for the taking of intimate samples with consent.

In July 1999 the Home Office published Proposals for Revising Legislative Measures on Fingerprints, Footprints and DNA samples. This consultation document formed the basis for some of the measures included in this Bill.

The Bill allows all lawfully taken fingerprints and DNA samples to be retained and used for the purposes of prevention and detection of crime and the prosecution of offences. This arises from the decisions of the Court of Appeal (Criminal Division) in R v Weir and R v B (Attorney General's reference No 3/199) May 2000. These cases raised the issue of whether the law relating to the retention and use of DNA samples on acquittal should be changed.

In these two cases, compelling DNA evidence that linked one suspect to a rape and the other to a murder, could not be used, and neither suspect could be convicted. This was because, at the time the matches were made, both defendants had either been acquitted or a decision made not to proceed with the offences for which the DNA profiles were taken. Currently, section 64 of PACE specifies that where a person is

Continued on page 16