RJT 37

Summary

This report has been prompted by the government's decision to table an amendment to the Crime and Immigration Bill, currently before the House of Lords, removing clause 129 from the Bill. The clause has the effect of increasing the penalties for those convicted in connection with the illegal disclosure and obtaining of personal data. The clause implements proposals originally put forward by the Information Commissioner. Its removal at this stage would have highly damaging symbolic and substantive consequences, especially at a time of such strong public and political concerns over breaches of data security.

This is the first legislative opportunity for the government to demonstrate how seriously it takes the safeguarding of personal information. Withdrawal of this clause at this advanced stage, when there has been no political opposition, may well be seen as a lack of priority for tackling the problems of security data and the need to reinforce data protection.

Background

Section 55 of the Data Protection Act, makes it an offence to obtain, disclose or procure the disclosure of confidential personal information knowingly and recklessly without the consent of the organisation that holds the information. In May 2006 the Information Commissioner presented a special report[1] to Parliament - **What Price Privacy?** - which exposed an extensive and lucrative illegal trade in confidential personal information. At the centre of the trade were networks of middlemen, often involved or associated with the private investigation industry. Their clients included private individuals, financial services companies, insurers, journalists, law firms and even local authorities. The suppliers and, in many cases, the customers involved in the trade were committing the offence at Section 55 of the Act.

The report presented real examples including:

- information obtained for a newspaper about the car and telephone calls of a family member of a celebrity;
- information obtained from the elderly mother of a insurance claimant by deception and then used to impersonate the claimant to obtain account information from his bank;
- a private investigator obtaining address details by deception from a medical centre in order to pass them to an abusive husband trying to track down his wife who had moved in order to start a new life.

[2 -3 more examples??]

The report documented at length how this illicit market works and – from material seized under search warrant powers by the Information Commissioner – included a tariff of prices charged for obtaining confidential telephone, criminal, vehicle and other records.

The report demonstrated that - although this has been a criminal offence for many years - the current penalty regime is too weak, often resulting in a derisory fine or conditional discharge which has not succeeded in stemming this illegal activity. Fundamentally the low penalties devalue the offence, mask the true seriousness of the crime and fail to have any significant

[1] The Information Commissioner, What price privacy?, HC1056, 10 May 2006

deterrent effect. The main recommendation of the report was the introduction of a possible two year prison sentence for those convicted of committing the Section 55 offence.

In December 2006 the Information Commissioner presented a follow up report[2] to Parliament detailing the progress made. There had been widespread support for the Commissioner's proposals. In particular the Information Commissioner particularly welcomed the government's recognition that the current penalties are too low and had launched a formal consultation exercise on raising the maximum penalty to include prison sentences. Further to that consultation the Government included clause 129 in the Criminal Justice and Immigration Bill to bring this reform into effect. The clause did not attract any attention at Second Reading in either House and was subject only to a probing amendment at Committee stage on the House of Commons.

Notwithstanding the lack of controversy during the legislative progress, there has been substantial positive Select Committee interest in the issue on the last 12 months:

- The Commons Culture, Media and Sport Committee's report on Press Self-Regulation [unequivocally supported the Commissioner's proposal] [Quote?].
- The Lords Science and Technology Committee's report[3] on Personal Internet Security (August 2007) urged the Government to look at the effectiveness of the Information Commissioner in enforcing good standards of data protection and recognised that amongst other problems faced by the Commissioner the existing penalties for offences are inadequate.
- The Commons Health Committee's report on the 'The electronic patient record'[4] (September 2007) welcomed the proposed custodial sentences when considering the necessary operational security of electronic patient records and underlined the need for effective enforcement. The security of electronic patient records was seen as essential to protect the privacy of patients and for them to trust that their confidentiality will be respected.
- On [ ] the Commissioner gave oral evidence to the Commons Home Affairs Committee about these issues at the opening session of their inquiry into a Surveillance Society.
- On [ ] the Commissioner gave similar evidence to the Lords Constitutional Committee at the opening session of their inquiry into the constitutional implications of a Surveillance Society.
- The Commons Justice Committee's Report on Protection of Personal Data noted [para 22] that the Criminal Justice and Immigration Bill increased penalties, but did not introduce new offences.
- On 14 January 2008 the Commissioner was invited to elaborate on the problems when giving oral evidence to the Joint Human Rights Committee's enquiry into recent data losses.

The need for tough sanctions has increased substantially since What Price Privacy?, the government's consultation exercise and consideration by Select Committees. The loss of 25 million records by HMRC (including some 7 million bank details) has focused on the substantial financial risks of identity theft. But this has also brought home the massive attraction to criminals able to obtain personal data of this nature. More than ever the threat of imprisonment is needed to deter those attempting to secure data illicitly, to deter insiders who may be tempted to disclose illicitly and more generally to demonstrate the seriousness of the offence.

[2] The Information Commissioner, What price privacy now?, HC36, 13 December 2006
[3] The Science and Technology Committee, Personal internet security, HL Paper 165-I, 10 August 2007
[4] The Health Committee, The [redacted]ronic patient record, HC422-I, 13 September 2007

Withdrawal of clause 129

The Commissioner fully understands the government's desire to secure rapid enactment of the Criminal Justice and Immigration Bill. However, removal of Clause 129 would send inexplicable and damaging signals soon after a series of data breaches. A legislative opportunity demonstrating the seriousness of safeguarding personal information would be reversed at a stroke. Removal of the clause would signal a lack of priority for tackling the problems of data security and the need to reinforce data protection:

- The primary purpose of increased penalties is to deter deliberate data breaches. This is aimed at staff inside organisations, at the private investigators who obtain data illegally, and at their various clients.
- There has been such strong support for the proposal from organisations which recognise the vulnerability of their data. The Chief Executive of the NHS Connecting for Health project, for example, has spoken about the benefits of a clear message to deter unauthorised disclosure of electronic health records. Other government departments have been victims of those illegally obtaining data which they hold.
- A reversal on sanctions for deliberate breach must seriously undermine the long overdue measures being taken to address accidental breaches. The Data Handling Review Team led by Sir Gus O'Donnell recognises that good data handling, especially data security, has not been taken seriously enough and that this is largely a leadership and cultural issue. To withdraw clause 129 - which has symbolic and substantive purpose - would significantly weaken the credibility of [the package of mandatory and advisory measures announced in the final report of Sir Gus's Review on [XXXXX].
- There is a widespread expectation amongst data controllers and their advisers that the stronger penalties will soon become law. The same is true within sectors which the Commissioner's report has identified as involved with the illegal trade in personal data - including investigators, financial institutions, law firms and journalists.
- Withdrawal would damage the reinvigorated credibility and authority of data protection law and the Information Commissioner's Office. Following an extensive consultation, the Commissioner's Data Protection Strategy spells out that stopping the illegal trade in personal data is a top priority.
- Public confidence in the protection of their data has already been damaged by high-profile data losses. Withdrawal would increase the risks for data sharing initiatives and would sit strangely with the Identity Cards Act which already has the identical sanctions against unauthorised disclosure.

Media Concerns

There have been concerns from some sections of the press that a custodial sentence would have a "chilling effect" on investigative journalism. Representations against the measure from media organisations have not been convincing. In effect, they are arguing against a criminal offence which has been on the statute book for many years. They object to tougher sanctions

against activities which they say do not exist or are not widespread. But the louder their protests against stronger penalties, the more it suggests questionable practices. The offence is only committed when there is deliberate or reckless disclosure of personal data without the consent of the organisation which holds it. The implication of their case is that they wish to be able to break the law.

No new criminal offence is being created and there is already a defence for journalists whose activities can be justified as being in the public interest. But they should be aware of the offence and think carefully before seeking to obtain personal information which is known to clearly confidential. As well as the explicit public interest defence, genuine investigative journalism will be protected by the Statement of Prosecution Policy which the ICO intends to adopt.

In his speech on Liberty on 25 October 2007, the Prime Minister acknowledged the concerns expressed in media circles, but made clear that he was not convinced by them. He stated that:

> *"Clear guidance will make sure that legitimate investigative journalism is not impeded* ***but the sanctions provide a strong deterrent to protect personal privacy****."*

A continuing market

There are indications that the Commissioner's reports and the government's proposals have already had at least a temporary effect in reducing this activity. Nevertheless the Commissioner continues to see evidence of the existence of an illegal trade in personal information and is investigating and prosecuting offences under Section 55 of the Act. Ongoing investigations involve information held by government departments, telecommunications companies, financial institutions and health trusts.

Cases resolved by the ICO since the initial report include:

- In April 2007 Infofind Ltd, a tracing company, and its managing director Nick Munroe pleaded guilty to 44 counts of illegally obtaining the personal information of hundreds of individuals held by the Department for Work and Pensions and selling it on to a finance company tracing debtors. In each case the people illegally obtaining the information impersonated DWP employees in order to gain access.
- [Other cases??]
- In addition there have also been 26 written undertakings and 7 cautions issued to other individuals and organisations since the follow up report was published.

Conclusion

People care about their personal information and have a right to expect that their personal details are and should remain confidential. Who they are, where they live, who their friends and family are, how they run their lives and their health and well-being - these are all private matters. Individuals may choose to divulge such information to others. In some situations, intrusion into their privacy may be necessary and permissible for public interest reasons. But

personal information held confidentially should not be available to anyone prepared to pay the right price.

Failure to respect an individual's privacy can lead to real distress and in some circumstances mental, physical and financial damage. At a time of increased information sharing it is essential that information is kept secure and that individuals trust that their privacy will be properly protected. Recent high profile security breaches in the public and private sectors have increased awareness of the importance of data protection amongst the public and will also have impacted upon the confidence they have in organisations respecting their privacy.

The Information Commissioner continues to believe that it is necessary for data protection offences at Section 55 of the Act to have a custodial sentence. The possibility of a prison sentence will serve as a deterrent for those that could dismiss a fine as a business overhead while making considerable profit from their illegal activity. If serious sanctions are not available to penalise deliberate breaches, there can be little hope that improvements to prevent accidental breach will be taken seriously.

The Information Commissioner is therefore extremely disappointed by the Government's intention to withdraw clause 129. This is a pernicious, and largely hidden, illegal market and the Commissioner is determined to stop it.

xx/0x/08