Introducing a custodial penalty for breaches of Section 55 of the Data Protection Act

An update from the Information Commissioner

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 and the Freedom of Information Act 2000. He is independent from government and promotes access to official information and the protection of personal information. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

The case for making available custodial sentences as the penalty for section 55 offences was overwhelmingly supported by respondents to the Department of Constitutional Affairs consultation "Increasing penalties for wilful misuse of personal information" in 2006. Indeed, at the time the Government itself recognised the case was overwhelming, and gave a commitment to introduce custodial sentences. This provision was introduced to Parliament during the passage of the Criminal Justice and Immigration Act 2008, but was amended at the report stage in the House of Lords so as to leave it up to the Secretary of State to commence the custodial sentence provision by statutory instrument. Section 77 of the Criminal Justice and Immigration Act (the custodial penalty) is accompanied by an enhanced 'reasonable belief' defence for the special purposes of journalism, literature and art (Section 78). Both sections remain to be commenced.

On 16 November 2009, I responded to a consultation from the Ministry of Justice entitled "Knowing or reckless misuse of personal data - introducing custodial sentences" which suggested the Government were ready to commence these provisions. My paper updated the state of play in relation to prosecutions under Section 55 of the Data Protection Act 1998 (DPA) and reiterated the case for introducing custodial sentences. This included the impending prosecution of two T-Mobile employees who were selling subscribers' contract details to rival mobile phone companies.

The Ministry of Justice has yet to issue a formal response to this consultation, but I am aware that the Department has been pursuing other measures to strengthen the otherwise somewhat weak deterrent in respect of Section 55 breaches. The Minister of State, Lord McNally, told delegates at the ICO's data protection conference in Manchester in March 2011 that the Government was urging the prosecution of Section 55 offences in the Crown Court where the fine can be unlimited. Confiscation under the Proceeds of Crime Act also provides a significant deterrent. The Sentencing Council was also being invited to communicate with the courts to advise on appropriate approaches to sentencing, stressing that Section 55 offences were no 'victimless crime'.

These measures are an advance, but not in themselves an adequate response to the problem. In my opinion, the case that the previous

administration found compelling in 2006 has only grown stronger over the past five years.

Deterrent effect

In response to the 2006 consultation, over 94% of respondents said that they welcomed the introduction of custodial penalties. This was because a custodial penalty would provide a deterrent effect as it would show the importance of data protection compliance and the seriousness of the offence. In the past five years, the importance of online records to almost every interaction the citizen has – with the state, local government, the NHS, DVLA, his/her bank, insurers, social networks – only makes the risks greater and the need for security and an effective deterrent greater still.

On 1 September 2009 an ex-member of the BNP appeared at Nottingham Magistrates Court in front of the District Judge. He pleaded guilty to unlawfully disclosing the BNP members list, contrary to Section 55. He was fined £200 and ordered to pay £100 costs. The District Judge commented "the fine was low because the defendant was on benefits" and "it came as a surprise to me, as it will to many members of the party (BNP), that to do something as foolish and as criminally dangerous as you did will only incur a financial penalty".

More recently, in passing sentence on 10 June 2011 in a case involving an employee of T-Mobile, who sold personal details of customers whose contracts were coming to an end, the Judge complained that his sentencing powers were limited and that any sums that could be raised by the defendants "would not reflect either of your true culpability".

Finance

There is a great pressure within the finance industry to obtain or confirm the current address for debtors. In the current climate of over indebtedness the number of those who are defaulting on debts is increasing and on top of this there is now a requirement on finance institutions to issue financial statements at least once a year even if an account is in default.

Other service providers, including local authorities and utility companies are also under pressure to ensure that monies owed are collected and all efforts are made to try and locate the whereabouts of absconded account holders.

As a result of this there is a substantial industry in the tracing and locating of individuals. The Credit Services Association estimates that in the region of 20 million trace enquiries are processed in the UK each year. It is clear from investigations and prosecutions carried out by the ICO that some of the techniques used within the tracing industry are criminal in their nature in that they would breach Section 55 of the Act. The preferred target of many of those "blagging" attacks are those organisations in the public and private sectors to which individuals have little or no option as to whether

they provide their personal details, such as DWP, HMRC, NHS and utility companies.

The average trace enquiry costs around £20-£25 and firms are offering 70-90% success rates. These search firms are often approached after the finance houses have already tried using the legitimate means deployed by their own tracing departments. This poses a real question as to whether search firms can genuinely offer such apparent value for money whilst only using lawful means to obtain personal information.

Insurance & Legal Professions

There is clear evidence that both the insurance and legal professions have used private investigators to obtain information which could not routinely be obtained otherwise, particularly information about the financial circumstances of claimants or defendants. The information is often obtained to support a legal process or to determine whether a legal process is practicable. The fact that a legal process is involved does not of itself give sufficient justification for the unlawful activity which is undertaken in order to obtain the information. There are legal gateways in both civil and criminal law whereby information can be lawfully obtained but at times these are circumvented by the use of private investigators who may revert to criminality in order to gather the required information.

Recently we have seen growing public concern over the activities of so called "ambulance chasers". Individuals receive unsolicited and often unwelcome approaches from businesses asking them if they have been involved in an accident and offering to pursue a compensation claim on their behalf, often on a supposedly "no win no fee" basis. Although it is clear that some of these approaches are made at random others appear to be targeted on those who are known to have been involved in an accident. This raises the question of how these businesses know who to target. In some cases it is clear that information about those who have been involved in accidents has been obtained as a result of Section 55 offences. We have recently brought a successful prosecution in a case where an NHS employee was passing confidential information from NHS records to her partner, who was being paid commission to supply the information to a personal injury claims management company. It is important that the sentences available to the courts in circumstances such as these truly reflect the harm that can be caused both to vulnerable individuals and to the organisations with which they entrust their personal information.

Certainty for organisations

It is widely accepted that employees are one of the biggest risk to information security. The Data Protection Act 1998 requires businesses and other organisations to invest in appropriate technical and organisational measures to prevent the unauthorised disclosure of personal information. However, by failing to provide an adequate deterrent to Section 55 offences, the Data Protection Act does not sufficiently support employers in discharging this responsibility. It is important that an adequate deterrent exists to help prevent businesses

and other organisations becoming the victim of a determined employee or contractor who sets out to compromise their security measures.

This is probably why support for custodial sentences is so great across the public and private sectors. Responsible organisations put a lot of effort into protecting personal data, but can see former employees walk away from court with only a small fine for selling or giving away personal information of their customers. In this context, commencing Sections 77 and 78 of the Criminal Justice and Immigration Act 2008 could be presented as a reduction in the regulatory burden on responsible private and third sector businesses by strengthening the support available to them and thereby helping them meet their obligations to keep personal information secure.

There is a discrepancy here between the public and private sector. Employees within the public sectors could find themselves charged with an offence of misconduct in a public office, whereas within the private sector the only option at present is a fine under the Data Protection Act.

If a custodial option was available under the Data Protection Act it would bring all employees within a sentencing regime which is both equitable and appropriate in today's information society.

It is worth noting that in the last three years the ICO has issued 16 cautions in circumstances where employees have abused their access rights to work related information and obtained information for their own personal use.

Public trust and confidence

One of the reasons given by Government in 2006 in support of custodial sentences was that the public needed to have trust and confidence in an age of data sharing initiatives, where both public and private sectors are collecting and exploiting ever greater volumes of personal information. Citizens and consumers need to have the assurance that their information is properly protected, and that those who abuse personal information will be appropriately punished.

With the current Government strongly promoting a "digital by default" agenda, it seems perverse to allow custodial sentences to sit on the statute books and not be commenced. We have already seen how large scale data losses contributed to a collapse in public trust and confidence relating to a range of initiatives brought in under the previous government. But with digital identity assurance, the collection of communications data, NHS reforms and the transparency agenda all demanding ever greater volumes and sharing of personal information, a large scale data theft close to the heart of Government could greatly undermine the Government's reform programme. This would be thrown into even sharper relief if any individuals prosecuted in connection with such a theft were to walk away from court with only a fine. The transparency and modernisation agenda would be strongly underpinned by the commencement of the custodial penalty regime.

The threat from organised crime

SOCA's latest "Threat Assessment" report includes a number of references to theft of personal data. The key extracts are:

"Alongside this increased use of technology, criminals have become more aware of the value of information, especially personal data, as a money making source. This has led to a growing criminal market for large volumes of personal data taken from vulnerable computer systems, which is traded and exploited in a range of frauds, and for the tools and techniques required to commit these offences.

- E-Criminality - A Criminal Market for Stolen Data

276 The driver behind the majority of data thefts is the profitability of compromised private information, particularly detailed financial information. Criminals compromising large quantities of data sell it either directly to those able to realise its monetary value through fraud, or to those who act as data brokers, aggregating data from different sources and selling it to other criminals. Internet crime has no "middlemarket" as it rarely requires the movement of a physical commodity. Criminals of all types and levels, including individuals looking to carry out small-scale, high-volume frauds are able to buy compromised private data directly from the primary sources.

277 Most of the data traded provides the means to access and defraud online accounts, or the ability to defraud payment card accounts using actual counterfeit cards or through card not present (CNP)22 fraud.

- UK Vulnerabilities to Data Theft

278 Individuals are targeted primarily for user names and passwords to enable criminals to access, and in some cases to control, online accounts, usually bank accounts but also other types, such as online brokerage accounts.

Individuals are also targeted for private details of their payment card accounts. This is achieved by tricking the account holder into revealing private data through fake emails and websites ("phishing") or by infecting the account holder's computer with malicious software ("malware") that automatically intercepts and forwards data to the criminal. Although public awareness of these threats is improving, the attacks are becoming increasingly sophisticated.

279 Centrally-held data typically consists of bulk payment card and identity data stored in a database. This data is targeted by criminal hackers who try to overcome security measures protecting the data so they can steal it in bulk."

We are also aware, from our conversations with the police, that they have concerns that unlawful methods are being used to obtain information

about jurors or witnesses, with a view to intimidating witnesses or members of the jury, or exerting other undue influence on criminal proceedings.

It is clear that SOCA do not consider the theft of personal data to be a less serious offence, and the fact that misuse of personal information features so prominently in their threat analysis would suggest that the unlawful trade in personal information is of growing interest to organised crime. Continuing to deny the courts the option of a custodial sentence in these circumstances is inconsistent with the threat identified by SOCA.

Alternatives

The recent T-Mobile case at Chester Crown Court was encouraging. For the first time, a confiscation order was imposed under the Proceeds of Crime Act. The ICO expects to be able to retain income from such orders and devote the additional resources to raising awareness and to enforcement. But such an approach is only relevant where the activity is on an almost industrial scale, perhaps over a period of a year or more, and involving large sums of money. It does not address the smaller scale incidents that may be of far greater significance to safeguarding privacy but which are not carried out for substantial financial gain – for example the BNP case.

The availability of a custodial penalty would also enable the ICO to bring prosecutions more speedily. Being able to interview under caution at the earliest stage would speed our investigations. Offences would be recorded on the Police National Computer, a significant factor for private investigators who otherwise regard a modest fine as a mere business cost, no more troubling than a parking ticket.

Proportionality

It is worth pointing out that while there will undoubtedly be some which will warrant a custodial sentence, there will continue to be many cases which are appropriately dealt with under current provisions. Custodial sentences would and should only be used in the most serious cases. Their primary function is to act as an effective deterrent both to those who might write off a fine as a business expense and to those who might successfully plead limited means in court and thereby avoid a meaningful fine.

This, again, was the view of Government in their response to the 2006 consultation. At the time sentencing guidelines were proposed to ensure that custodial sentences were only handed down where this was proportionate.

The availability of a custodial penalty would, however, open up the full range of sentencing, between a fine and a prison term. These would include community penalties, tagging and curfews – clearly more effective than fines in the case of small scale operators who very often appear in court as having 'little means', being on benefit, unemployed and so on.

The Fourth Estate

What is striking about the current scene is how little it involves the press or investigative journalism. The Commissioner's 2006 reports[1] certainly had a lot to say about the use of 'blagging' to access personal information in circumstances that might constitute a Section 55 offence (depending on whether a public interest case could be mounted.) But the 2006 reports highlighted a problem over enforcement that had general application and has only become more of a problem in the intervening years. The evidence around press behaviour arose because the ICO had raided, under Operation Motorman, a particular private investigator whose major customers were Fleet Street titles. The evidence was acquired in 2003 and even then related to historic transactions. The evidence of Section 55 breaches is all around us; but the ICO has no fresh evidence involving the press and, consequently, nothing to add to what we said in 2006.

The Section 78 enhanced defence involving 'reasonable belief' looks to me to provide adequate reassurance that investigative journalism will not be adversely affected, even where enquiries establish that a journalistic hypothesis does not in the end stack up.

Lord Justice Leveson will be taking evidence about what happened in 2003 and subsequently. That should not prevent the Government and Parliament from acting to address the 'modern scourge' of Section 55 crime that affects ordinary citizens to an ever greater extent – and Fleet Street hardly at all.

Conclusion

The more I review the evidence of the misuse of personal information and the more I see the numbers of reported cases rising the greater becomes the harm to those individuals whose privacy is intruded on and to those organisations that are targeted by unlawful activity. The case for custodial sentences becomes ever more unanswerable, as does the urgency of finding an early way forward.

Christopher Graham
Information Commissioner

August 2011

[1] What Price Privacy? and What Price Privacy Now?