



Information Commissioner's Office

THE INFORMATION COMMISSIONER'S RESPONSE TO THE MINISTRY OF JUSTICE CONSULTATION PAPER ON THE KNOWING OR RECKLESS MISUSE OF PERSONAL DATA: INTRODUCING CUSTODIAL SENTENCES.

1 INTRODUCTION

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 Information Commissioner welcomes the opportunity to comment on the proposals in the MoJ consultation paper, 'The Knowing or Reckless Misuse of Personal Data: Introducing Custodial Sentences.' His responses to the consultation questions are set out briefly below. He then goes on to provide further examples of the continuing illegal market in personal data in support of his answers.

2 RESPONSE TO THE CONSULTATION QUESTION

1 Should the Secretary of State introduce custodial penalties for offences committed under section 55 of the Data Protection Act 1998 (DPA);

Yes, the Information Commissioner continues to believe that custodial penalties are necessary if the law is to provide an effective deterrent against the illegal trade in personal data.

2 Subject to the responses to Question 1, whether the custodial sentences should be set at the maximum available under the power (ie twelve months imprisonment on summary conviction and two years imprisonment on indictment);

The Information Commissioner is of the view that the custodial sentences need to be set at the maximum available under the power in order to have the necessary deterrent effect.

3 Subject to the responses to Question 1, whether the Government should bring in the new custodial penalties from April 2010, when the ICO is provisionally being given enhanced powers;

The Information Commissioner agrees that the Government should bring in the new custodial sentences from April 2010.

4 Subject to the responses for Question 1, whether the additional defence for anyone who can show that he was acting for special purposes (as defined in section 3 of the DPA) with a view to publishing journalistic, literary or artistic material, in the reasonable belief that the obtaining, disclosing or procuring was in the public interest should be introduced alongside the increased penalties.

The Information Commissioner understands the reasons for the additional defence and agrees with it.

In support of his answers to the above questions the Information Commissioner sets out below the background to his response, how this is informed by the wide range of activity in the illegal market in personal data and his conclusions.

3 THE CASE FOR INCREASED PENALTIES.

Since the Data Protection Act 1998 (DPA) became law in 2000, the Information Commissioners Office (ICO) has received a steady stream of complaints from individuals who have reported that their privacy has been breached. Investigations by the ICO and the police uncovered evidence of a widespread and organised undercover market in confidential personal information. This illegal activity was subject to two reports, 'What Price Privacy?' and 'What Price Privacy Now?' which were presented to Parliament in May and December . The first report, 'What Price Privacy?' called on the then Lord Chancellor to bring forward proposals to raise the penalty for persons convicted on indictment of section 55 offences to a maximum of two years imprisonment, or a fine, or both; and for summary convictions, to a maximum six months imprisonment, or a fine or both. The aim of this call was to attack the undercover market in personal information and also to send out a clear signal that obtaining personal information unlawfully is a serious crime.

'What Price Privacy' outlined several investigations which had previously been carried out by ICO investigators into allegations of the unlawful obtaining of personal information. The main case was Operation Motorman. This was a case where a private investigator had been supplying personal information to some 305 journalists. The personal information included details of criminal records, registered keepers of vehicles, driving licence details, ex-directory telephone numbers, itemised telephone billing and mobile phone records. Documentation seized at the home of the private investigator included reports, invoices, settlement of bills between the detective and many of the better known national newspapers – tabloid and broadsheet.

Following the publication of 'What Price Privacy?' the ICO began a consultation with interested parties. The result of the consultation was reported six months later in the second report 'What Price Privacy Now?' The Government also commenced a consultation on introducing prison sentences for the offence of unlawfully obtaining personal data.

The penalty for section 55 was not increased immediately, but section 77 of the Criminal Justice and Immigration Act 2008 gave the Secretary of State the power by order to introduce custodial sentences, for unlawful obtaining etc of personal information. The Information Commissioner believed then that custodial sentences were needed and continues to do so. The evidence that follows supports this position.

At present the offence of unlawful obtaining etc is not a recordable offence. It is not therefore recorded on the Police National Computer. Fingerprint impressions, DNA samples and descriptive details are not currently taken from those individuals who are prosecuted by the ICO for the section 55 offence (a descriptive form contains personal information relative to the accused person, for example, ethnic appearance, build, shoe size, glasses, hair, facial hair, marks, scars and abnormalities etc). If the penalties for this offence are increased to imprisonment the offence will become a recordable offence. This will not only underline the serious nature of the offence but will ensure that those convicted carry a meaningful criminal record.

The Extradition Act 2003 implemented, amongst other things, the framework for European arrest warrants. This facilitated the extradition, from one European country to another, of individuals who had committed an offence listed on the European framework list. One set of listed offences includes computer crime. An offence under section 55 of the Data Protection Act, punishable with two years imprisonment on indictment, could well fit into this category.

Therefore, should the penalty for unlawful obtaining etc be increased to imprisonment it may be possible to extradite individuals for this offence from foreign jurisdictions. Given the ease with which personal data can be moved across borders and accessed worldwide and the possibility of those engaged in unlawful obtaining etc operating from outside the UK this is likely to become increasingly important. As the law stands, without the status of 'recordable offence' some practices could go unpunished because the perpetrators are outside the jurisdiction.

4 INVESTIGATIONS INTO SECTION 55 OFFENCES BY THE ICO.

The ICO investigations unit investigates in the main offences contrary to section 55 of the DPA 1998. Operation Motorman (the investigation which led to the publication of 'What Price Privacy?' and 'What Price Privacy Now?') was perhaps the most high profile case in recent years but there have been other significant investigations where individual privacy has been breached and where individuals have been caused serious harm and distress. Whilst Operation Motorman uncovered widespread apparent¹ abuse by journalists, the media are not the only or even the main offender. Many others are involved in the unlawful obtaining of personal information.

¹ In the absence of any information about the stories that were being pursued, the Information Commissioner cannot say whether a public defence might have been persuasive.

Those who wish to obtain personal information unlawfully in the main do so for financial gain. In this digital age there are many organisations in the public and private sector which hold huge amounts of information on many millions of individuals. There is no doubt that this personal information has a monetary value. As the following cases illustrate there are now many criminals and unscrupulous individuals who have realised that there is money to be made in the unlawful obtaining and selling of personal information. There are many different levels of unlawful obtaining. At the lower end of the scale there are cases of private investigators and tracing agents attempting to obtain current address details of debtors. At the other end there are private investigators supplying personal information to criminals who are of interest to the Serious and Organised Crime Agency. What is clear is that the current penalty for the offences of unlawful obtaining etc has only a limited deterrent effect upon those committing these offences. The potential rewards are great. As things stand, the risks are low.

ICO investigators have in the past investigated cases where private investigators or tracing agents have been tasked to locate debtors. In their search for the current address of a named debtor they will often approach government departments which are likely to hold up to date information on individuals. For example, the Department for Work and Pensions and Her Majesty's Revenue and Customs are often a target of the 'bogus caller.' The caller will use many different tactics to obtain information. Often they will say that they are the person of interest and attempt to obtain unlawfully information. On other occasions they will purport to be an employee of the organisation or department which holds the data. They will have an in depth knowledge of the structure of the organisation and the type of jargon used. On occasions they will also be aware of an employee's unique reference number and their internal telephone extension numbers. They will often be aware of other information such as the reorganisation of a department or the move by employees to new premises. They use snippets of information like this as an icebreaker to convince the person they are calling of their in depth knowledge of the organisation or department. This assists the bogus caller to convince the individual they are talking to of their legitimacy. Within the 'trade' the bogus callers are known as 'blaggers'.

'Blaggers' are also often interested in the financial standing of individuals and will also attempt to obtain personal information unlawfully from banks and building societies. Other information of great interest to the blagger is itemised billing from telephone and mobile telephone records. Telephone service providers are targeted routinely by the bogus caller.

Medical records are another rich vein of information for the blagger. General practitioner surgeries and hospital medical records departments are also routinely targeted. The risks can only become greater as, in the interests of patient care, health records are increasingly networked and potentially made available to a wide range of health professionals.

In the past, ICO investigators have come across 'Blaggers Manuals' when searching suspect premises. The manuals give detailed advice on the types of

uses to use when attempting to obtain information unlawfully from a myriad of organisations in both the public and private sector.

5 INFOFIND LIMITED.

In January 2005, a member of staff at the Department of Work and Pension call centre (DWP) received a call from a person purporting to be another employee of the DWP. The call centre employee believed the bona fides of the caller and during the call the employee disclosed to the caller details of the addresses of eight individuals. A subsequent check with these individuals revealed that one had recently been contacted by a finance company about an outstanding debt.

Enquiries with the finance company revealed that they had put the eight individuals who were subject of the bogus call, "out to trace". This is the industry term for asking private investigators etc to try and locate the current address for a person. The organisation asked to trace the outstanding debtors was called Infofind limited

A short time later another employee of the DWP received a similar call to the one above and during the call they disclosed details of a further 42 individuals. The release of the data was not an indication that the call centre employee was inexperienced or naïve but demonstrated the skill of the bogus caller. The same finance company later confirmed that that the 42 individuals were of interest to them as debtors. They said that they had passed the details of the individuals to a firm of solicitors who had asked Infofind to trace them.

Further calls were made to the DWP and during those calls the details of 200 other individuals were passed to the bogus callers bringing the total number of items of personal information obtained to 250. The individuals who were the subject of these calls were customers of another finance company who had put the details of these further 200 individuals out to trace with Infofind. It was established that Infofind charged £20 per successful trace.

The owner of Infofind Limited, was interviewed under caution but declined to answer any questions relating to the calls made to the DWP and how he subsequently came into possession of the information obtained during those calls.

However, from information obtained from other sources it became clear that there was an individual operating within the tracing industry that used a particular modus operandi to obtain information from the DWP and this information was then sold back to tracing agents who then sold it on to the finance institutions.

On 25 October 2005, the owner of Infofind Limited was later fined a total of £3,200 and was ordered to pay £5,000 towards prosecution costs. The Information Commissioner believes that fines such as these do little to deter a highly profitable business.

6 PEARMAC LIMITED.

In November 2003, the ICO became aware that telephone calls had been made to the family of a rape victim attempting to obtain her current address and contact

telephone numbers. Telephone calls were also made to her GP and her utility company. In the call to the utility company her bank account details were disclosed and in the call to the GP there was an attempt to obtain her medical records. These calls were traced to the offices of Pearmac Limited in London.

ICO investigators executed a search warrant at the premises of Pearmac. They were greeted at the premises by, an individual who had a previous conviction for a section 55 offence, with the following comments.

“What’s the maximum fine for this, £5000? I will write the cheque out now”

When interviewed the owner declined to disclose who had hired him to obtain the personal information relating to the rape victim.

The conduct of Pearmac Limited led to the individual believing that the attempts to obtain her private details could be a part of an act of revenge directed at her for reporting and giving evidence against her attacker (who was imprisoned for six years). Further, the intrusion into her private life led her to have to seek medical advice in relation to a stress related illness.

On 10 November 2004, the defendant was subsequently fined a total of £6,250 + £600 costs for four counts of unlawfully obtaining personal information and three counts of attempting to obtain personal information.

The victim later commented that the fine handed down was derisory and further commented “It’s maddening really, for people who commit this crime to just receive a miniscule fine. I do think it is wrong”

It was clear from this case that the private investigator had little interest in the motive of the individual who paid for his services. In similar cases individuals who obtain personal information are not concerned about the motive of the individual asking for the information only the amount of money that the information is worth. There is little evidence of bloggers addressing motive even when it appears clear that the motive may be to cause harm to an individual.

7 RELEASE OF THE BRITISH NATIONAL PARTY (BNP) MEMBERSHIP LIST.

In December 2007 the BNP circulated a membership list (“the list”) to selected party members to be used only for specified party purposes. Following an internal dispute, two BNP members left the party. Both individuals had possession of the circulated list of members. Between 12 and 18 November 2008 the membership list was posted on the internet and was made publicly available without the consent of the BNP. The list contained the names, addresses and contact details of the party members. An allegation of an offence contrary to section 55 of the DPA was made to Dyfed Powys Police (DPP) after a meeting between the ICO and DPP it was decided that there should be a joint investigation into the leaking of the membership list. After making enquiries DPP identified the Internet Protocol (IP) address of the computer from which the list had been uploaded onto the internet. Further enquires revealed that the computer was situated in the home address of one of the two members who had left the BNP and who had been in possession of the membership list.

A search warrant was obtained by the Information Commissioner's Office, to search the home address of this individual. During the search of the premises a laptop computer and two memory sticks (secreted within a corn flakes box) were recovered. A subsequent forensic examination of the laptop computer led to the reconstruction of deleted files which showed that the computer was linked to the 'blog' website on which the membership list was posted.

On 1 September 2009 one of the ex-members of the BNP appeared at Nottingham Magistrates Court in front of the District Judge. He pleaded guilty to unlawfully disclosing the list, contrary to Section 55 DPA 1998. 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 too 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".

8 POLICE FORCES.

It is not just the ICO which investigates and prosecutes offences contrary to section 55 of the DPA. Most professional standards departments of police forces in the UK are at some time or other investigating police officers and police staff for the unlawfully obtaining etc of personal information contained on police computer systems. Not surprisingly the majority of these investigations are focused on the misuse of the Police National Computer (PNC).

On 26 August 2009, a Crown Court judge in Chelmsford, Essex, commented that it was astonishing that he could only fine an Essex police staff member for breaches of the Data Protection Act. The individual concerned had accessed Essex Police intelligence systems unlawfully on some eight hundred occasions. He unlawfully accessed the police systems from January 2007 to November 2008. Amongst other things, he passed on mobile telephone records, checked up on his housemate's two sisters and accessed the record of another man's arrest. He was subsequently fined £750.

On 15 November 2008, a police constable in Norwich stopped a motor car which he observed committing a traffic offence. He spoke to the driver of the vehicle and also checked the driver's details on the Police National Computer (PNC). As a result of what was said to the officer in respect of some intelligence on the PNC about the driver of the car the officer searched the vehicle. The following day the driver of the vehicle contacted Norfolk Police and said that a friend of his, who was a serving police officer, had checked the PNC on his behalf and had told him the details of the source of the information that was held about him. He also named the constable who had helped him. The constable was subsequently arrested and charged with the section 55 offence. He appeared at Norwich Magistrates Court on the 17 February 2009 and was fined £2,500.

On 29 January 2007, a 79 years old man died shortly after a brick was thrown through the window of his home in Derby. The deceased had been involved in a dispute with a 26 year old woman over a car parking space at a local supermarket four days prior to his death. The husband of the woman, after being told about the dispute decided to exact revenge on the pensioner. He asked a

serving police officer to obtain the address of the pensioner from his vehicle registration number. The police officer retrieved the address details from the PNC which he gave to the husband. The husband and his brother went to the pensioner's home and threw the brick through the window. They were both later convicted of manslaughter. The police constable was convicted of the section 55 offence and was fined £1,200. He resigned from the force.

Over the past twelve months or so the West Midlands Police has prosecuted three members of staff for unlawfully accessing personal information held on police systems. A serving police constable obtained information from force intelligence systems and then passed this to a relative who was involved in a case of assault against the data subject. In a second case a custody office assistant with access to the PNC conducted a number of checks in relation to non police related matters. These matters were investigated and she later tendered her resignation. She later appeared at Coventry Magistrates Court. A third officer was charged with eighteen offences of unlawfully obtaining personal information. This related to information held on the PNC and Force Intelligence Systems. He pleaded guilty to these offences at the Magistrates Court and was referred to the Crown Court for sentence. He resigned from the force.

9 MOBILE TELEPHONE SELLERS.

A mobile telephone service provider brought to the attention of the ICO evidence to suggest that employees were selling customer data. This included subscriber details, relating to customer's mobile phone contracts and their contract expiry dates. It was alleged that the information was being sold on to competitors of the service provider who were using the information to cold call customers prior to the expiry dates of their mobile phone contracts with the service provider to offer them an alternative contract. The service provider alleged that many thousands of customer account details had been unlawfully obtained.

An ICO investigation indicated that the information had been sold on to several brokers. Subsequently several search warrants were obtained and executed.

A prosecution case is now being prepared and until the case comes to court no more details can be released. However the number of records involved runs into the millions and it appears that substantial amounts of money changed hands.

10 CREDIT REFERENCE FILES.

A credit reference agency recently reported to the ICO that 41 consumer credit files had been accessed by individuals who were not the subject of the files and who had no authority to access the files. An investigation by the agency revealed that those who had successfully obtained the credit files had initially attempted to gain access via the company's website. When they failed to pass the on line checks they proceeded to the manual verification stage where copies of identity documents such as passports and driving licences were requested. The identity documents forwarded to the credit reference agency appeared to be authentic and the individuals were allowed access to the credit files. Closer examination revealed that the identity documents were forgeries. They were described as 'high quality counterfeit documentation'. This example of the

unlawful obtaining of personal information demonstrates the lengths that criminals are prepared to go to obtain personal information. Clearly the information contained in a credit reference file would allow many different kinds of mischief when in the wrong hands. Because those responsible have not been apprehended their motive is not known.

11 CONCLUSIONS.

The Information Commissioner wishes to make it clear that the purpose for the call to increase the penalty for the section 55 offence is to act as a deterrent to those who are currently involved in the unlawful trade in personal information. As this consultation response has shown there are many individuals who seek to unlawfully obtain personal information for a myriad of motives. It is clear that the current penalty for the offences of unlawful obtaining etc has only a limited deterrent effect upon those committing these offences. In many cases a fine alone will be looked on by the offender as little more than a business expense or simply as a risk worth taking.

Under the law as it stands, there is a public interest defence for section 55 offences. The Information Commissioner notes that the defence available to Journalists would be strengthened under the proposal for a custodial sentence.

It is clear that an effective deterrent to the section 55 offence is needed. More and more personal information is being collected and held by government, public authorities and businesses. In the future, as new systems are developed and there is more and more interconnection of these systems, the risks of unlawful obtaining and disclosure become even greater. If public trust and confidence in the proper handling of personal information, whether by government or by others, is to be maintained effective sanctions for unlawful obtaining etc are essential.

Custodial sentences will underline how, in an era of ever increasing collection, storage and use, unlawful obtaining etc is regarded as a serious offence. They will also have the added benefit of making the section 55 offence a recordable one and open up the possibility of extradition in appropriate cases.