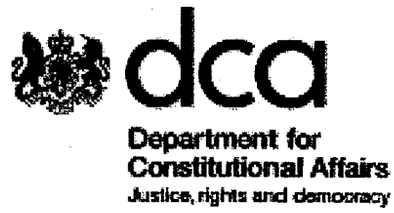


Increasing penalties for deliberate and wilful misuse of personal data

Response to Consultation
CP(R) 9/06
07/02/2007

Response to consultation carried out by the Department for Constitutional Affairs. This information is also available on the DCA website at www.dca.gov.uk

Increasing penalties for deliberate and wilful misuse of personal data
Summary of responses

Contents

Increasing penalties for deliberate and wilful misuse of personal data
Summary of responses

[leave this page blank – back of contents page]

Increasing penalties for deliberate and wilful misuse of personal data
Summary of responses

Introduction

This document is the post-consultation report for the consultation paper, 'Increasing penalties for deliberate and wilful misuse of personal data.'

It will cover:

- the background to the report;
- a summary of the responses to the report;
- a detailed response to the specific questions raised in the report; and
- the next steps following this consultation.

Further copies of this report and the consultation paper can be obtained by contacting **Carl Pencil** at the address below:

Information Rights Division
Department for Constitutional Affairs
6th Floor Selborne House
54-60 Victoria Street
London
SW1E 6QW

Telephone: 020 7210 8034
Email: carl.pencil@dca.gsi.gov.uk

This report is also available on the Department's website at: www.dca.gov.uk

Increasing penalties for deliberate and wilful misuse of personal data
Summary of responses

Background

The Consultation Paper 'Increasing penalties for deliberate and wilful misuse of personal data' was published on 24 July 2006. It invited comments on proposals to increase the penalties available to the courts under section 55 of the Data Protection Act 1998 (DPA) to enable those guilty of offences to be imprisoned for up to 2 years on indictment and up to 6 months on summary conviction.

Section 55 (4-8) of the DPA make it an offence to sell or offer to sell personal data which has been (or is subsequently) obtained or procured knowingly or recklessly without the consent of the data controller. Section 60 of the DPA provides for prosecutions and penalties.

The Information Commissioner's Special Report to Parliament "*What price privacy? The unlawful trade in confidential personal information*"[1] (*What price privacy?*) highlighted the extent of the illegal trade in personal information and the corrosive effects that this has on society. Investigations by the Information Commissioner's Office (ICO) and the police uncovered evidence of a widespread and organised undercover market in personal information. In one major case, the evidence included records on information supplied to 305 named journalists working for a range of newspapers.[2] The Report recommended custodial sentences for offences relating to the misuse of personal data. The follow up report "*What Price Privacy Now? The first six months progress in halting the unlawful trade in confidential personal information*"[3] (*What Price Privacy Now?*) reviewed the progress and the responses received by the ICO.

The Government agrees with the ICO that the current financial penalties available to the court do not act as a sufficient deterrent to those engaged in the illegal trade in personal information.

Currently section 60 provides for:

- On summary conviction, a fine not exceeding the statutory maximum (currently £5,000); and

---

[1] HC 1056, 10 May 2006.
[2] What price privacy? The unlawful trade in confidential personal information. P17.
[3] HC 36, 13 December 2006.

- On conviction on indictment, to a fine (which is unlimited.)

Greater data sharing within the public sector has the potential to be hugely beneficial to the public as individuals and to society as a whole. The benefits of data sharing include reduced administrative costs for businesses and the public sector, increased efficiency and more effective targeted and personalised services. The Government's vision is to ensure that information will be shared to expand opportunities for the most disadvantaged, fight crime and provide better public services for citizens and business, and in other instances where it is in the public interest. The "*Information sharing vision statement*" sets out our vision for better, more customer-focused services supported by greater information sharing which will protect and support individuals and society as a whole.[4]

The Government is strongly committed to ensuring that there is robust protection for personal data. That is why the Government is proposing that the penalties available to the court should be increased.

The Government proposes to amend section 60 of the DPA to allow for, in addition to the current fines:

- Up to 6 months imprisonment on summary conviction (increased to a maximum of 12 months imprisonment in England and Wales when s154 of the Criminal Justice Act 2003 comes into force, and in Scotland when s35 of the Criminal Proceedings etc. (Reform) (Scotland) Act 2007 comes into force); and
- Up to 2 years imprisonment on indictment.

The consultation paper sought views on whether:

- Custodial penalties should be available to the courts when sentencing those found guilty of offences under section 55 of the DPA.
- Custodial penalties would act as an effective deterrent to those who unlawfully trade in and otherwise deliberately or recklessly misuse personal information.
- The length of the proposed penalties is appropriate/ proportionate.
- A guideline issued by the Sentencing Guidelines Council is necessary for the offence in England and Wales.

[4] DCA 47/06 HM Government: Information sharing vision statement, 13 September 2006

Increasing penalties for deliberate and wilful misuse of personal data
Summary of responses

The Consultation period closed on the 30 October 2006 and this report summarises the responses, including how the consultation process influenced further development of the proposals. This consultation is in line with the Code of Practice on Consultation, issued by the Cabinet Office.

A list of respondents is at Annex A.

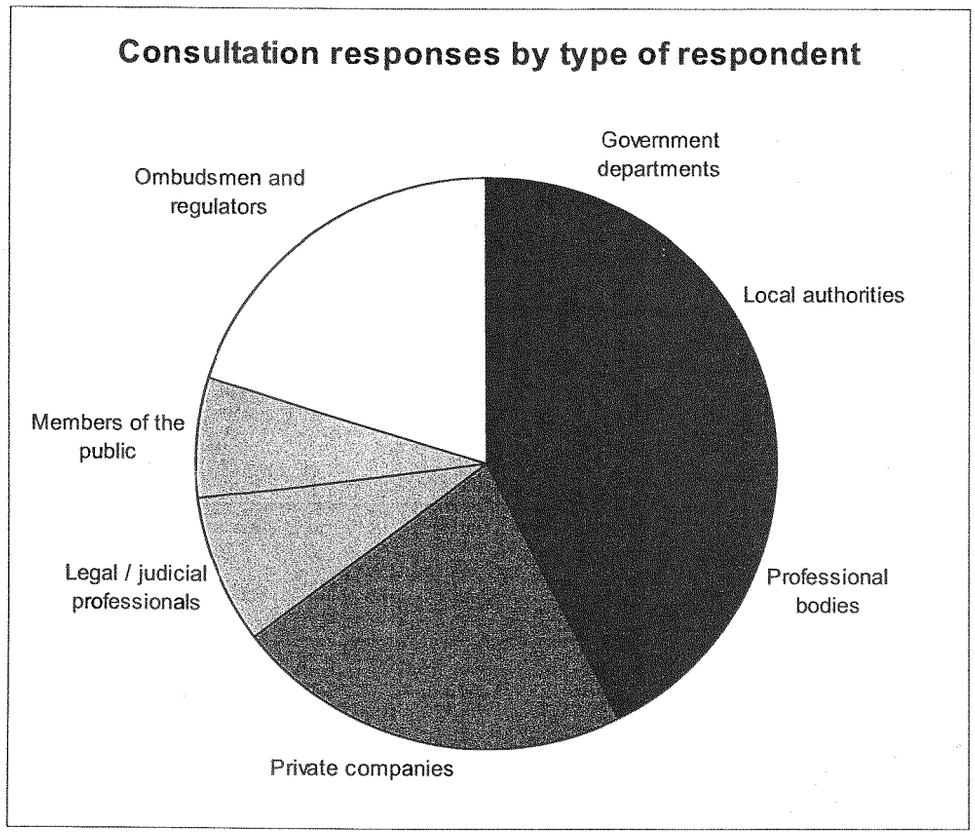
Summary of responses

We received a total of 63 responses including three nil returns from the Faculty of Advocates, Ministry of Defence (MoD) and Ofgem.

Respondents included Government departments, local authorities, professional bodies, private companies, legal practitioners/ judiciary, and Ombudsmen/ independent regulators. The different categories of respondents are illustrated in Figure 1 and the responses are broken down by respondent type in Table 1 below. Some respondents did not answer all the questions so the combined totals per question are less than 63.

Figure 1: Pie chart of respondent type

This pie chart illustrates the breakdown of consultation responses by respondent type.



Increasing penalties for deliberate and wilful misuse of personal data
Summary of responses

Table 1: Table of respondent type to the consultation paper: Increasing penalties for the deliberate and wilful misuse of personal data

	Number of respondents who agreed/ disagreed							
	Question 1		Question 2		Question 3a/3b		Question 4	
Respondent type	Agree	Disagree	Agree	Disagree	Agree	Disagree	Agree	Disagree
Govt. dept.	7	0	7	0	6	1	7	0
Local authority	5	0	4	1	3	2	5	0
Professional body	12	1	11	2	10	3	11	2
Private co.	11	2	10	3	9	3	10	3
Legal	5	0	5	0	4	0	3	2
Public	4	0	3	1	3	1	2	2
Ombudsman / regulator	12	0	12	0	12	0	10	1
TOTAL	56	3	52	7	47	10	48	10

*Some respondents did not specifically answer all questions provided in the consultation paper. Inferences have been made from general comments where possible. All figures provided are therefore a best assessment of the questions addressed by respondents.

In summary the responses were as follows:

- Respondents generally welcomed the introduction of custodial penalties to provide a larger deterrence to potential offenders, to provide public reassurance that offenders would receive the appropriate sentence, and to achieve parity with a number of disparate pieces of legislation, which deal with similar types of offences.

- The majority of respondents agreed that custodial penalties would be an effective deterrent because it would demonstrate the legal importance of data protection compliance, and the seriousness of the offence. Many respondents also highlighted the importance of enforcement when considering deterrence. A few respondents did not agree with the proposal and argued that unlimited fines were more appropriate.

- Many respondents agreed with the proposed length of custodial sentence and that the courts should have access to the same sanctions as it would for similar offences. A minority of respondents argued that a maximum sentence of twelve months on summary conviction and five years on indictment would be more effective.

- The majority of respondents agreed that a guideline would be necessary to ensure consistent sentencing policy, and that prison was reserved for the most severe breaches of the Act. The Magistrates' Association stated that if offences increase in the future, it might be useful to have a starting point for the average type of offence with indicators of mitigating and aggravating features. However, the Council of Circuit Judges disagreed with this proposal and stated that there was a need for flexibility in sentencing to account for the variety of circumstances, and that guidelines tended to be perceived as rigid.

- The Newspaper Publishers Association, the Newspaper Society, the Periodical Publishers Association, the Scottish Newspaper Publishers Association and the Society of Editors provided a joint response - to be referred to as the "press group" response - which generally opposed the proposals. Guardian News & Media (GN&M) attached an additional submission, which supported the press group's opposition to custodial sentences but took a different view of some of the issues discussed.

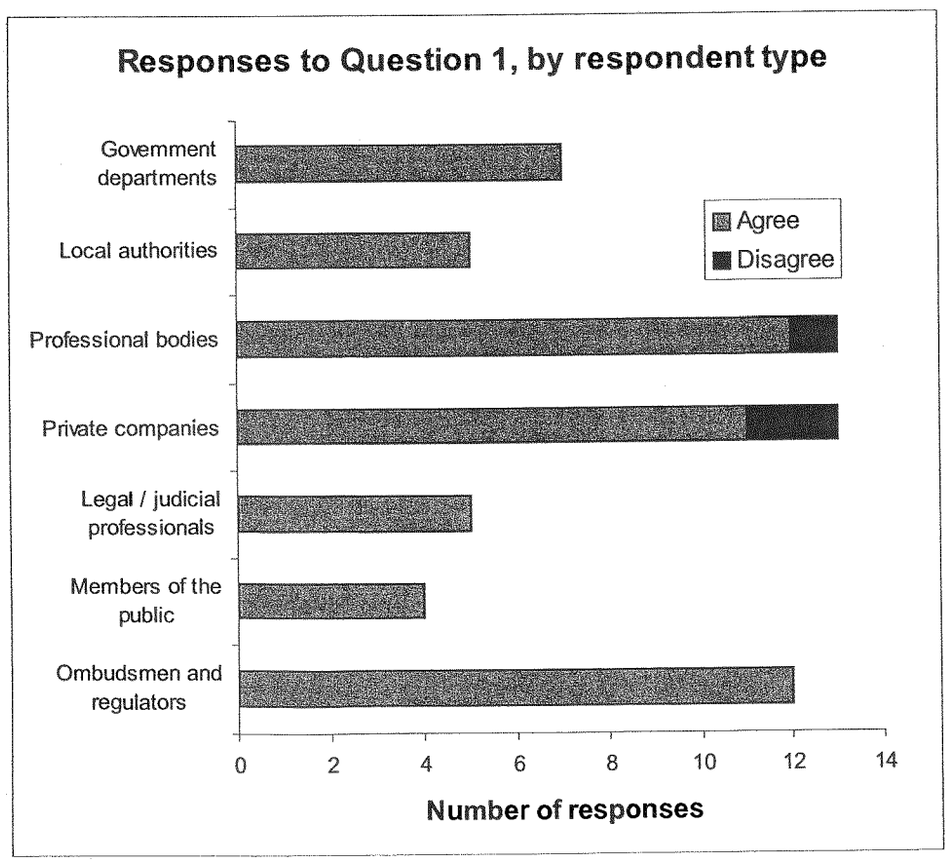
Responses to Specific Questions

Question 1: Do you agree that custodial penalties should be available to the court when sentencing those who wilfully abuse personal data (i.e. knowingly or recklessly obtain, disclose or seek to procure the disclosure of such data without the consent of the data controller?) Please give reasons for your answer.

The majority of respondents agreed that custodial penalties should be available to the court when sentencing those who wilfully abuse personal data.

The numbers of respondents who agreed and disagreed with this proposal, according to respondent type are illustrated in the chart below.

Figure 2: Graph of responses to question 1 by respondent type



The main reasons given for this view were to increase deterrence, compliance with the Data Protection Act, consumer trust and confidence and the alignment of the Act with legislation for similar offences. This is in accordance with the reasons as set out in the Consultation Paper, which stated the following:

The Government therefore believes it is necessary to increase the penalties available to the courts for three reasons:

- In order to provide a larger deterrence to those who seek to knowingly or recklessly disclose or procure the disclosure of confidential personal information without the consent of the data controller,
- To provide public reassurance that those who are successfully prosecuted may, dependent on the gravity of the offence, be sent to jail.
- To achieve parity of approach across a number of disparate pieces of legislation which deal with similar type of offences.[5]

Deterrence

The Information Commissioner's Report "*What Price Privacy?*" highlighted the scale of the illegal trade in personal information and the substantial financial profits earned. In one case an agent was earning up to £120,000 per month.[6]

A significant number of respondents agreed that fines were not currently deterring potential offenders from engaging in such a potentially profitable trade. Many respondents felt that the penalties, which are currently available for the misuse of personal information (i.e. statutory maximum fine of £5,000 on summary conviction and an unlimited fine on indictment) do not accurately convey the serious nature of the offence. The Direct Marketing Association stated its awareness of a view in the industry that compliance with the Data Protection Act is not a high priority because the penalties for breach are not as significant as under other legislation. Some respondents commented that the offence should be seen in the same light as burglary or theft, which carry custodial sentences.

---

[5] Increasing penalties for deliberate and wilful misuse of personal data. P10
[6] What price privacy? The unlawful trade in confidential personal information. P25.

Many respondents also stated that there was a need for tougher penalties due to an increased need to deter this type of crime. As more data is held and exchanged between public sector bodies, the opportunities for those seeking to either sell or illegally gain access to this data increase. The Royal Academy of Engineering commented that the proposal must also be seen in light of general moves towards e-Government and measures such as ID cards, which will necessitate the storage of a large amount of valuable data. Therefore there must be more serious consequences for those who attempt to fraudulently access this valuable data. The Government is committed to ensuring that there is robust protection for personal data.

The inclusion of custodial penalties as a sentencing option will also demonstrate that the Government is serious about the enforcement of Data Protection legislation and that the courts will prosecute offenders and impose custodial penalties for serious breaches of the law. The Government is clear that prison should be reserved for serious, violent and dangerous offenders. Those responsible for large scale abuse of personal information or repeat offenders are more likely to receive custodial sentences than those engaged at a lower level.

The Association of Chief Police Officers (ACPO) also supports the introduction of custodial penalties. They stated that there needs to be a strong deterrent and that the suggested custodial penalties will demonstrate this tougher stance. The Crown Prosecution Service (CPS) strongly supports this proposal and shares the view that the increased penalty will send out a signal that unlawfully obtaining personal information is a serious crime and will act as a deterrent.

Public/ consumer confidence

One of the aims of the Government's wider strategy on data sharing is to increase public confidence in the sharing of personal data. The Government is keen to make the most effective use of the information that it holds and to promote the sharing of personal data across the public and private sector to increase efficiency, and develop more effective targeted and personalised services.

There have been increasing concerns about the apparent increase in the trade of personal information and identity fraud. It is therefore essential for people to be confident that their personal data will not be wilfully or recklessly abused. Ernst & Young stressed that the effect on individuals of the wilful abuse of their personal data is potentially very damaging and amounts to an infringement of their human rights. The Serious Fraud Office (SFO) also remarked that a lack of public

confidence in data management affects the public willingness to support initiatives relating to increased data sharing. Consequently it is imperative that appropriate sanctions prevent the abuse of data and ensure the security of personal information.

The introduction of custodial penalties will demonstrate to the public that the Government is committed to securing the safety and integrity of personal information. A number of respondents agreed that the proposals would help to underpin and strengthen public confidence in the Government's data sharing strategy.

Aligning legislation

The Data Protection Act 1998 is the central piece of legislation, which governs how personal data should be processed. The consultation paper underlined various pieces of legislation such as the Identity Cards Act 2006, Social Security Administration Act 1992 and the Commissioners for Revenue and Customs Act 2005 which imposed custodial sanctions for the misuse of personal information in particular circumstances.[7]

The DPA should set the standard for offences relating to the wilful misuse of personal information, and the courts should have access to the same sanctions as they would have for similar offences. The majority of respondents agreed that this would lead to a consistent approach and parity between the prosecution of offences committed under the Act and similar offences under other legislation.

Three respondents disagreed with the proposal that custodial penalties should be available to the court when sentencing those who wilfully abuse personal data.

The press group argued that unlimited fines in the Crown Court were adequate, and that there were four reasons why they believed the imposition of custodial sentences to be incompatible with the European Convention on Human Rights (ECHR). Their reasons were that the ICO and the Government had not made a case for criminal penalties; the Government had not demonstrated that there was a pressing social need to interfere with Article 10 rights; the measures were disproportionate to the problem of a market in personal data (if it existed) and there were other criminal and civil remedies available to protect data subjects.

---

[7] Increasing penalties for deliberate and wilful misuse of personal data. P13.

Bisnode asserted that the DPA was not suited to the introduction of custodial penalties and that the purpose of prevention and rehabilitation would not be served by a custodial sentence. They suggested that, if necessary, the court could award custodial sentences for related offences e.g. obtaining services by deception, or bribery. The respondent recommended increasing fines and enabling the courts to seize property as proceeds of crime whenever possible.

Bisnode recommended amending court guidelines to give more weight to these offences and argued that this would ensure that the courts take these offences more seriously, instead of increasing custodial sentences.

The third respondent, Acxiom was concerned at the escalation of the sanction and stated that there was no justification or need to increase the level of sanction due to the insignificant number of successful prosecutions and the fact that the average fines imposed were within the current limits.

The Government's response to these points is as follows:

The Government believes that the current financial penalties (which include unlimited fines) are not sufficiently deterring offenders from engaging in the illegal trade in personal information. The ICO's report "*What Price Privacy?*" made the case for the introduction of criminal penalties. It highlighted the extent of the trade and the profits earned. The Government believes that it is therefore necessary to increase the penalties available to the court to deter potential offenders. A significant number of respondents agreed that custodial penalties were necessary.

This sentencing option is available in several pieces of legislation designed to protect the confidentiality of information. The DPA is the overarching piece of legislation, which governs how personal data should be processed, and it should therefore be aligned with legislation for similar offences (to allow for comparable sanctions). In response to the point that there are other civil and criminal remedies available to protect data subjects, it is arguable that these remedies have only been pursued in relation to data protection offences because the custodial sanction is currently unavailable under the DPA.

"What Price Privacy?" illustrated the extent of non-compliance with section 55 of the DPA and provides evidence that the existing penalties are not sufficiently protecting the rights of individuals. It reported that 305 journalists had been identified during Operation Motorman as customers driving the illegal trade in

confidential personal information.[8] The specific publications were identified in "*What Price Privacy Now?*"[9] Whilst condemning the trade in confidential information via private investigators, GN&M stated that the report contained striking prima facie evidence that many national newspapers may be habitually breaking the law by paying private detectives for information about people in public life and those associated with them.

The wilful abuse of personal data is an interference with a person's right to a private and family life under Article 8 of the ECHR; the Government is under an obligation to take steps to protect this right. The Government believes that the increased penalties are proportionate to the problem and necessary to protect this right and obligations of confidentiality. The Government does not accept that the offences under section 55 of the DPA will inevitably engage the right to freedom of expression under Article 10 of the Convention. For example, the mere fact that a journalist wishes to obtain information from a public authority or company does not in itself mean that Article 10 is engaged. However, if the proposed new penalties do interfere with that right, the Government believes that this would be justified. Article 10(2) recognises that the right to freedom of expression "carries with it duties and responsibilities." It permits restrictions that are prescribed by law and that are necessary in a democratic society for, amongst other things, "the protection of the reputation or rights of others" or "preventing the disclosure of information received in confidence."

The Government considers that these increased penalties strike an appropriate balance between the rights under Article 8 and Article 10, and that they are justified and proportionate. Lord Wakeham (in his role as chairman of the Press Complaints Commission) commented on this issue during the Data Protection's Bill's Second Reading in the Lords. He said "the Bill steers a sensible path which avoids the perils of a privacy law and achieves the crucial balancing act of privacy and freedom of expression in a clever and constructive way."[10]

The Government's response to the remaining points: The aim of sentencing is to punish the offender, reduce crime, rehabilitate the offender and protect the public. There is a range of sentencing options available to the court depending on the type, seriousness and circumstances of the case and the maximum penalty available by law. The Government is proposing that the courts have the option of

---

[8] What Price Privacy? The unlawful trade in confidential personal information. P17.
[9] What Price Privacy Now? The first six months in halting the unlawful trade in confidential personal information. P9.
[10] Official Report, HL, 2 Feb 1998; Vol 585, c.462.

custodial penalties available to them in addition to the current financial penalties and community sentences when sentencing offenders for the abuse of personal data. The Government agrees that there should be guidelines for the sentencing of this offence.

It is open to the court to impose a custodial sentence for any related offence as appropriate, and the courts can currently make orders for the recovery of property obtained through unlawful conduct. The powers available in relation to the proceeds of crime are discussed in further detail in the following section.

Other issues raised

When answering this question some respondents raised important issues, which are discussed below.

Liability of directors

One respondent queried whether a custodial sentence would be appropriate when the offence was committed by a business where the liability for the offence attached indirectly, or vicariously, to a director, manager or officer responsible for the running of that business or for authorising the processing activity.

The respondent who supported the proposals expressed concern that there was a remote possibility that an employee who acted unlawfully in carrying out the business of that organisation could inadvertently expose directors or officers to prosecution in addition to attracting liability themselves. This is of particular relevance due to section 61 of the Data Protection Act.

Section 61(1) of the DPA states that:

"Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent of or connivance of or to be attributable to any neglect on the part of any director, manager, secretary or similar officer of the body corporate or any person who was purporting to act in any such capacity, he as well as the body corporate shall be guilty of that offence and be liable to be proceeded against and punished accordingly."

The DPA requires data controllers to take steps to protect the security of any personal information, which they hold. The employer is therefore responsible for ensuring that there are adequate rules and procedures in place and that they are followed.

Many statutes, which create offences punishable by imprisonment, contain provisions in similar terms to section 61(1). The Government considers it appropriate that a corporate officer who consents or connives in the commission of an offence under section 55, or to whose neglect the commission of the offence is attributable, should in appropriate circumstances face the same penalties as those

who carry out the actions which constitute the offence. We therefore believe that the DPA currently carries appropriate liability for directors.

Property obtained through unlawful conduct

A number of respondents also recommended the use of the Proceeds of Crime Act 2002 (POCA). The Act gives the Crown Court the power to make confiscation orders if certain conditions are satisfied and if the prosecution asks the court to do so, or if the court believes it is appropriate. In summary, a confiscation order can be made if the defendant has benefited from the particular criminal conduct of which he/she has been convicted or from general criminal conduct, and will be an order requiring him/her to repay the benefit he/she has gained so far as is possible.

One respondent suggested that a freezing order might be a better deterrent. The purpose of a freezing order is to preserve the defendant's assets while claims are litigated in court, in circumstances where it is feared that the defendant would dispose of these assets or put them out of the successful claimant's reach. However, it is only an interim measure.

Under Part 5 of POCA, the Asset Recovery Agency (ARA) can bring civil proceedings in the High Court to recovery property that is or represents property obtained through unlawful conduct (civil recovery). The ultimate effect of the order is that, if the court finds that the property was obtained through unlawful conduct, it will make a recovery order. Monies received by ARA from the enforcement of the order are paid into the Consolidated Fund.

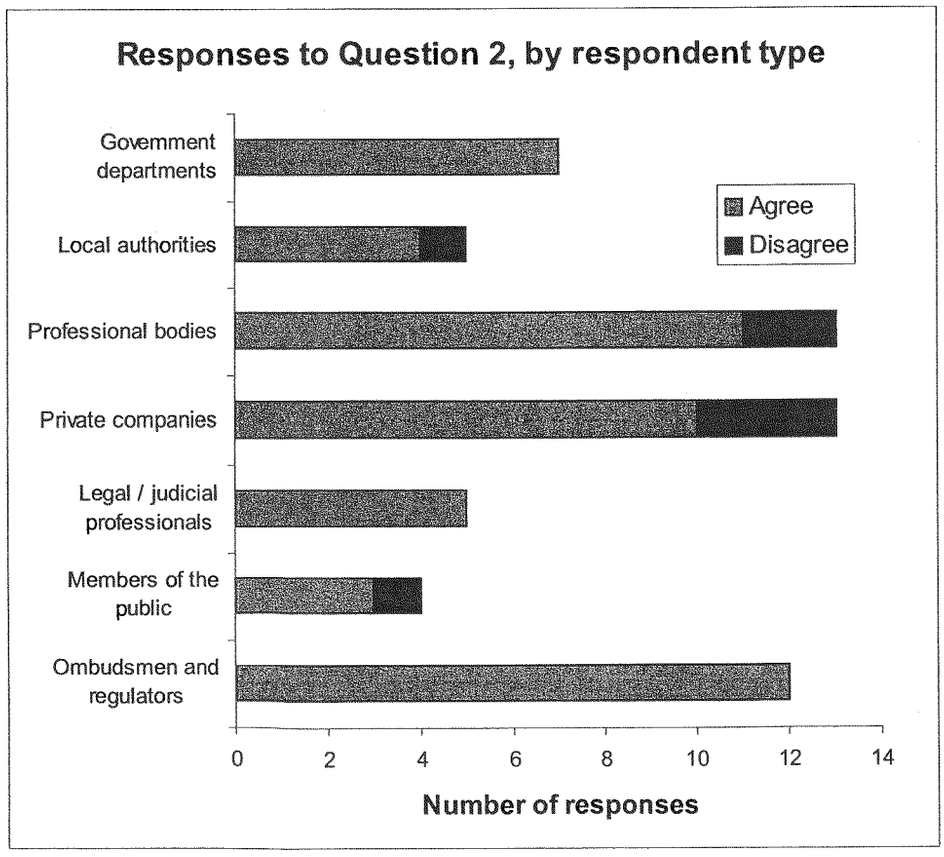
In summary, the power to make a confiscation order can be used on conviction for DPA offences; and a civil recovery order can also be sought in respect of the proceeds of unlawful conduct, which includes such offences. The ICO is aware of these options and considers whether they are appropriate for each case. The CPS also considers confiscation in any successful prosecution as part of their standard business processes.

Question 2: Do you agree that custodial penalties will be an effective deterrent to those who seek to procure or wilfully abuse personal data (i.e. knowingly or recklessly obtain, disclose or seek to procure the disclosure of such data without the consent of the data controller?) Please give reasons for your answer.

In answering question 1, many respondents cited deterrence as a main reason for the introduction of custodial penalties. Subsequently most respondents agreed that custodial penalties would be an effective deterrent, when replying to this question.

The numbers of respondents who agreed and disagreed with this proposal, according to respondent type are illustrated in the chart below.

Figure 3: Graph of responses to question 2, by respondent type.



Custodial sentences are the ultimate deterrent sentence that the courts are able to use. It is envisaged that custodial penalties will be used for the most serious offenders who are engaged in the large-scale abuse of personal data. In addition

the courts will be able to sentence offenders to suspended sentences, (except Scotland) community sentences and licence conditions. These are all more onerous than simply fining offenders and the Government believes that they will be a greater deterrent to those engaged in the trade in personal information than the current punishments.

One respondent commented that custodial sentences are more appropriate when there are significant financial rewards because custodial penalties cannot be easily set off against business earnings whereas fines can be included in charges for information and incorporated into the costs of the business.

Several respondents stated that the introduction of custodial sentences would confirm the **legal importance** of data protection compliance and demonstrate that the courts take the offence seriously. Another respondent said that the proposal would convey the message that the processing of personal data without consent is a crime and not just unethical. A couple of respondents also pointed out that individuals who leak information from their place of employment would be deterred from disclosing information due to the effect that a conviction would have on their ability to gain future employment.

However, a significant number of those respondents who agreed that custodial penalties would be an effective deterrent highlighted that **enforcement** was a crucial factor. If potential offenders conclude that custodial sentences are exceptional and believe that the potential high rewards are worth taking the risk, then they will not be deterred from committing these offences. Some respondents also recommended naming and shaming offenders and publicising cases on the ICO website to increase the general profile of the misuse of data offences, enhance deterrence and encourage compliance.

The Government agrees that enforcement is an important factor. The public should be confident that penalties are applied appropriately and consistently. CIFAS stated that the key to the success of the new penalties is apprehending, prosecuting and sentencing offenders. The level of deterrence will therefore increase in line with the risk of detection.

A minority of respondents stated that custodial penalties would not be an effective deterrent to those who seek to procure or wilfully abuse personal data.

The press group argued that the introduction of custodial sentences would have a profound chilling effect on free speech and seriously curtail legitimate investigative journalism. They argued that a journalist cannot always determine at the start of an

investigation whether the obtaining or disclosing or procuring of the information was justified as being in the public interest. GN&M said that "there is simply no guarantee that a court, looking at a situation with the benefit of hindsight, will share a reporter's view of what was "necessary" and/or in the "public interest," at the time of publication." They further argued that journalists would err on the side of caution rather than risk a custodial sentence, which would result in the non-publication of important stories on matters of public interest.

The Government's response: The Government has no wish to curtail legitimate and responsible journalism, and does not consider that the proposed penalties would have that effect. The Government is not seeking to change the definition of the offences, or of the defences which may be available to journalists, and is not aware of section 55 having caused any problems such as those described by the press group since the Act came into force. As the Information Commissioner has recently stated:

"There is no suggestion that the action of a journalist or private investigator in seeking information from public sources or friends and neighbours to pursue a story should be made illegal. However, journalists (and many others) who either directly or through middlemen obtain personal information from public and private sector organisations by bribery, impersonation and similar means are engaging in conduct which, unless they can clearly demonstrate a public interest, has quite rightly been illegal since 1994."[11]

Section 55 only applies where a person knowingly or recklessly obtains personal data without consent. Like other people, journalists can rely on the defences in section 55(2)(b) and (c), namely that they reasonably believed that they had the right to obtain the data or that they reasonably believed that the data controller would have consented, had he known that the data was shared.

The public interest defence in section 55(2)(d) is an additional defence. The public interest would be assessed in relation to the time the offence was committed. While there is no guarantee that the court would agree with a journalist about the public interest, the court would consider the public interest in obtaining data without consent on the day and in the circumstances in which the data were obtained. If the journalist had good reason to obtain data without consent, that would be relevant. In theory, a journalist could have a public interest defence for obtaining data to investigate an important story, even though the story later turned out to be

[11] What Price Privacy Now? The first six months in halting the unlawful trade in confidential personal information. P10.

unimportant or factually questionable, so that it was not in the public interest to go on and publish the data.

During the Parliamentary debates for the Data Protection Bill, the issue of reconciling privacy and freedom of expression was discussed. Mr George Howarth, the then Parliamentary Under-Secretary of State for the Home Department spoke about the relevant clauses in the Bill. He said "all the measures are intended, ...to protect journalists' right to handle material about people provided that it is for true journalistic purposes and in the public interest...they ensure that there are remedies for an individual where the privacy of information about them was in fact invaded."[12]

While the proposed penalties are intended to strengthen the protection of individuals' right to respect for their privacy, the Government considers that the current definition of the offences and the current defences in the DPA will strike the right balance between freedom of expression and privacy. This is in line with the European Convention on Human Rights and the Data Protection Directive.

It should also be noted that the Information Commissioner has signalled a desire to work with the Press Complaints Commission and Code of Practice Committee of Editors. He has engaged directly with the Chairman and Secretary of the Code of Practice Committee of Editors, and discussed the possibility of amending the Editors Code of Practice and suggested changes to the Code. Unfortunately, however, no concrete proposal has been brought forward and the Committee has not agreed to the suggested changes.[13]

Two respondents commented about the penal system. The Security Industry argued that custodial penalties did not successfully deter offenders from committing other crimes so only some would be deterred. ACPO added that it appears that the prison system is unable to support the custodial process.

Another respondent concluded that the fear of prison sentence may deter some but recommended the further exploration of how existing sanctions could be applied more effectively including the imposition of increased fines that are more commensurate with the offence being committed.

---

[12] House of Commons Standing Committee D, 21 May 1998.
[13] What Price Privacy Now? The first six months in halting the unlawful trade in confidential personal information. P19.

The Government's response: The aim of sentencing is to punish the offender, reduce crime, rehabilitate the offender and protect the public. There is a range of sentencing options available to the court depending on the type, seriousness and circumstances of the case and the maximum penalty available by law. Custodial sentences are the ultimate deterrent sentence that the courts are able to use. It is worth noting that a two-year custodial sentence will be the *maximum* available penalty and it will only be given where considered appropriate by the courts.

The Government is proposing that the courts have the option of custodial penalties available in addition to the current fiscal penalties, when sentencing offenders for the abuse of personal data. We would consider that those responsible for the large scale abuse of personal data, or repeat offenders would be more likely to receive a custodial sentence or a community order than those engaged at a lower level where a fine would be a more appropriate punishment.

A court is required to pass a sentence that is commensurate with the seriousness of the offence. The formulation and introduction of sentencing guidelines will also help to ensure a consistent sentencing policy and that available sanctions are applied effectively.

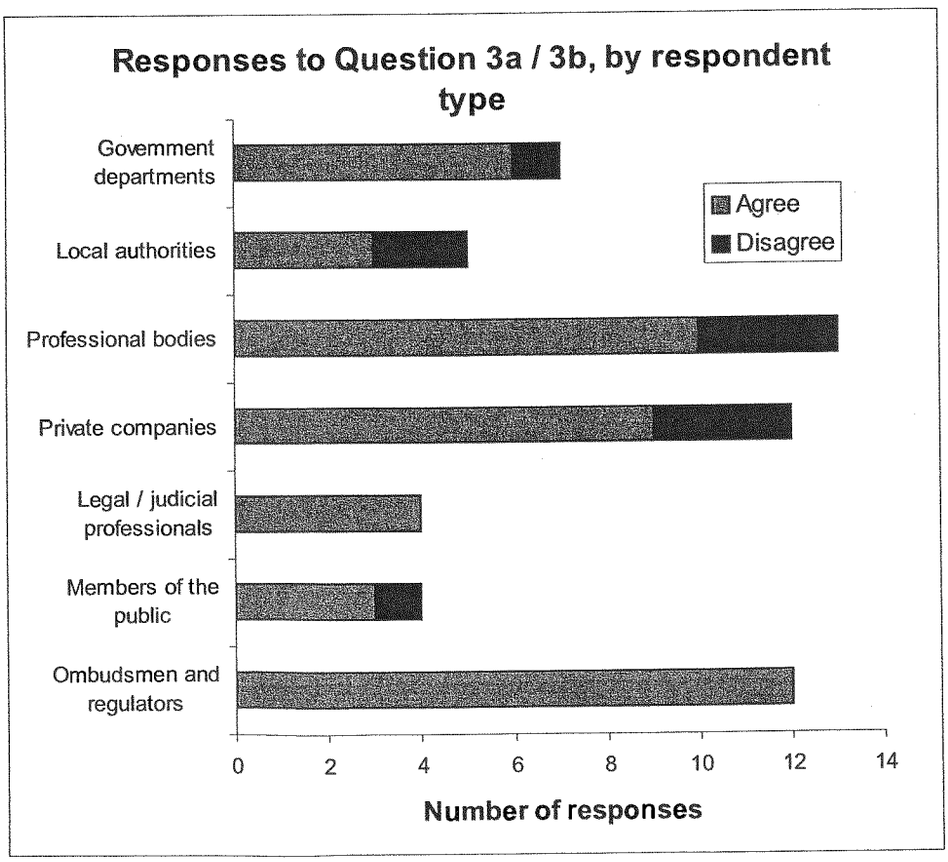
Question 3(a): Do you agree that the custodial penalties are of the right length? (Answered with question 3(b) below)

Question 3(b): If not, why not, and what do you suggest should be the maximum custodial penalty available to the courts (a) on summary conviction and (b) on conviction on indictment?

The majority of respondents agreed that the custodial penalties were of the right length.

The numbers of respondents who agreed and disagreed with this proposal, according to respondent type are illustrated in the chart below.

Figure 4: Graph of responses to question 3a and 3b, by respondent type.



The DPA is the central piece of legislation, which governs how personal data should be processed. It should be the piece of legislation, which sets the standard

for offences relating to the wilful misuse of personal information. It is therefore only right and proper that it should enable the courts to have access to the same sanction for the misuse of data as it would have for other similar offences.

The Government proposes to amend section 60 of the DPA to allow for, in addition to the current fines:

- Up to 6 months imprisonment on summary conviction (increased to a maximum of 12 months imprisonment in England and Wales when s154 of the Criminal Justice Act 2003 comes into force and in Scotland when s35 of the Criminal Proceedings etc. (Reform) (Scotland) Act 2006 comes into force); and
- Up to 2 years imprisonment on indictment.

The majority of respondents agreed that the length of sentence proposed was appropriate and proportionate. The main reason cited was to align the DPA with the various pieces of other legislation for similar type offences. Consequently all offenders would be subject to the same penalties to achieve consistency and parity. A number of respondents also stressed that the length of custodial penalties should reflect the seriousness of the level of abuse or misuse of data or the damage or distress caused to the individual. Consistent sentencing would also increase deterrence and the public's confidence in enforcement, that offenders are being apprehended and sentenced appropriately and according to the seriousness of the offence.

The Law Society of Scotland queried whether there would be different levels of penalties between Scotland and England when s154 of the Criminal Justice Act 2003 came into force. The Criminal Proceedings etc (Reform) (Scotland) Act 2007 will make similar provisions to the Criminal Justice Act 2003 – wherever an either way offence[14] is currently punishable with less than 12 months imprisonment, the maximum penalty will increase to 12 months.

---

[14] "Either way" offences are dealt with either by the magistrates or before a judge and jury at the Crown Court. A suspect can insist on their right to trial in the Crown Court. Similarly, magistrates can decide that a case is sufficiently serious that it should be dealt with in the Crown Court - which can impose tougher punishments.
www.cjsonline.gov.uk/the_cjs/how_it_works/magistrates_court/index.html

The Financial Services Authority agreed with the proposals and stated that they were similar to section 352(2) of the Financial Services and Markets Act 2000 for the misuse of "confidential information" (as defined in section 348). A person guilty of an offence is liable on summary conviction to a term of imprisonment not exceeding three months, or a fine not exceeding the statutory maximum or both, and a term not exceeding two years or a fine or both on conviction on indictment.

Some respondents disagreed with the proposed length, and felt that a longer period would be more effective. It should be noted that some respondents did not support their views with reasons. APACS stated that two years was consistent with the ID Cards Act 2006; however, a failure to report POCA disclosures carries a maximum sentence of five years. They stated that further alignment was needed. A few respondents including Privacy Laws & Business and the Institute for the Management of Information Systems (IMIS) suggested a longer penalty when the offence was linked to a more serious offence e.g. fraud, extortion, terrorist activity. IMIS argued that the proposed length of sentence would be too lenient, unless it was complemented by unlimited fines and additional prosecution when direct links to serious offences were proven.

A few respondents including South Holland District Council and Greenwich Council suggested a maximum sentence of twelve months on summary conviction and five years on indictment. Greenwich Council stated that cases have to be determined on an individual basis and should be dependent on the hardship and financial cost that the perpetrator has caused. One respondent recommended a maximum of three years on summary conviction and five years on indictment because few offenders actually serve the full term and short terms will not deter potential offenders.

Leicester Partners NHS stated that they preferred low custodial terms coupled with creative penalties, and suggested ten years on indictment for serious cases.

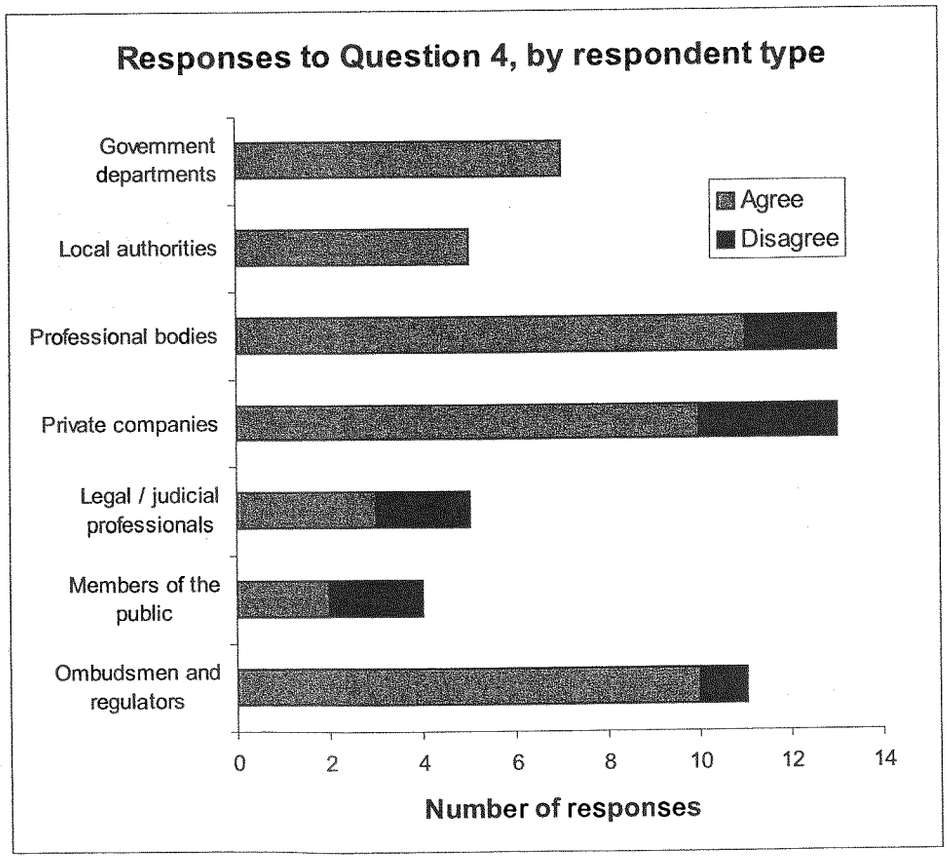
The Government's response: A number of pieces of legislation currently allow for custodial sanctions for the unlawful disclosure of personal data. The DPA needs to be amended to allow for comparable sanctions and ensure that it deals with offences for the misuse of data to the same standard. A maximum sentence of six months on summary conviction and two years on indictment is consistent with other legislation.

Question 4: Do you agree that a guideline issued by the Sentencing Guidelines Council is necessary for this offence in England and Wales?

The majority of respondents agreed that a guideline issued by the Sentencing Guidelines Council was necessary for this offence in England and Wales.

The numbers of respondents who agreed and disagreed with this proposal, according to respondent type are illustrated in the chart below.

Figure 5: Graph of responses to question 4, by respondent type.



The Sentencing Guidelines Council (SGC) produces sentencing guidelines in conjunction with the Sentencing Advisory Panel (SAP). The SGC receives advice from the SAP on a particular sentencing topic and uses this to formulate sentencing guidelines. These draft guidelines are published, consulted on and then revised. It is worth noting that the SAP consults statutory consultees and the wider

public as part of their research process. Final sentencing guidelines are then issued, and ready to be used by sentencers.

The guidelines:

- Encourage consistency in sentencing throughout the courts of England and Wales.
- Support sentencers in their decision making.

Any guidelines that are issued by the SGC must be followed or the judge or magistrate sentencing the offender must give reasons if they depart from them. The Sentencing Guidelines Council then keeps the guidelines under review so that they can be amended and developed as required.[15]

The Government's priorities are the delivery of sanctions that effectively reduce re-offending, punish and rehabilitate the offender and reassure the public. A guideline would include the **full range of sentencing options**, which are available to the court. The courts have a range of sentencing options available depending on the type, seriousness and circumstances of the crime and the maximum penalty available by law. The Finance and Leasing Association (FLA) stated that the courts must make use of the full range of sentencing options.

Available non-custodial sentences include fines and community sentences. Community sentencing combines punishment, reparation and decreasing the likelihood of re-offending. The Association of British Insurers (ABI) commented that there was scope for making full use of community sentences. Community sentencing is often a better option if an offender does not pose a great threat to the public. Community sentencing is also more likely to rehabilitate offenders and encourage reparation (two of the principles of sentencing) because it combines punishment with changing offenders' behaviour and making amends.[16]

The aim of sentencing is to punish the offender, reduce crime, rehabilitate the offender, protect the public and ensure that the offender makes reparation where possible. The Government is clear that prison should be reserved for serious, violent and dangerous offenders. ABI was reassured of the Government's commitment and stressed the importance of using custodial sanctions sparingly.

---

[15] www.sentencing-guidelines.gov.uk
[16] www.homeoffice.gov.uk/justice/what-happens-at-court/sentencing/#named3

The majority of respondents agreed that a guideline was necessary. Most respondents emphasised that this would ensure a **consistent sentencing policy**, appropriate sentence lengths and that prison was reserved for the most severe breaches of the law. The Information Commissioner has also highlighted that the proposals do not call for the creation of a new offence. A further safeguard is that only the Information Commissioner or the Director of Public Prosecutions may bring a prosecution.[17] The Health Safety Executive agreed that this should provide reassurance that prosecutions are only taken when warranted.

It is also noted that the Crown Prosecution Service (CPS) applies the Code for Crown Prosecutors to ensure that fair and consistent prosecution decisions are made. Prosecutors must consider whether there is sufficient evidence for each case, and if so, whether a prosecution is in the public interest.

Privacy Laws & Business highlighted that the DPA was a national piece of legislation so it was therefore important to avoid regional variations.

A number of respondents also felt that a guideline was necessary because of the **nature of data protection offences**. One respondent commented that the range of activities, which are considered an offence under section 55, might vary tremendously. Others stated that the circumstances giving rise to prosecutions will vary in gravity and complexity so it is important to have guidelines to ensure that the level of penalty is proportionate to the gravity of the offence. Individuals who make innocent mistakes should be treated proportionately. In contrast, the SFO commented that guidelines would be useful but stated that the range of behaviour within the offence is not such that it would be unduly difficult for a judge to sentence appropriately without guidelines. Bisnode stated that the guidelines should reflect the seriousness of the offences as outlined in the ICO's report, and commented that the information industry would benefit from more accurate sentencing.

One respondent stated that **the courts** are often criticised for lenient sentencing so guidelines must reflect the seriousness of the crime and the damage caused to the individual. It is common for guidelines to address issues such as the extent to which harm has been suffered. HMRC highlighted the importance of public confidence stating that the introduction of guidelines is likely to decrease inconsistency and enhance the desired deterrent effect. Due to the small number

---

[17] What price privacy now? The first 6 months in halting the unlawful trade in confidential personal information. P27.

of prosecutions, a couple of respondents, Privacy Laws & Business and D-Pap stated that guidelines should help the courts appreciate the significance of the offence and ensure a clear understanding of privacy infringement. OFCOM and DfES stated that it was important for courts to be supported in decision making.

The Magistrates' Association was in general agreement with the proposals. However, they stated that there were a small number of prosecutions, so specific guidelines might not be necessary. Nevertheless they stated that guidance from the SGC could be useful and if offences increase in the future, it might be useful to have a starting point for the average type of offences with an indication of mitigating and aggravating features. Socitm Consulting added that guidance would be welcomed should the implementation of penalties be subject to query.

Some respondents disagreed with the proposal that a guideline issued by the Sentencing Guidelines Council was necessary for this offence in England and Wales.

In answering this question, the press group argued that if the proposal were implemented then the DPA would need serious amendment to extend the journalistic exemptions in section 32 to breaches of section 55. "In other words, an honest belief by a journalist that he or she is acting in the public interest should be a defence to any offence which carries a prison sentence."

The Government's response: Sections 55 and 32 of the DPA are different in numerous respects. Section 32 gives media organisations exemption from some parts of the Act, which apply to them as data controllers. It provides media organisations or journalists (as data controllers) with an exemption from most of the data protection principles, and certain other provisions of the Act if they reasonably believe that, having regard to the special importance of the public interest in freedom of expression, publication would be in the public interest. This exemption applies to the processing of personal data with a view to the publication of any journalistic, literary or artistic material. The exemption excuses the data controller from complying with the provisions which he/she reasonably believes are incompatible with the purposes of journalism. It does not provide journalists with an exemption from civil liability.

However, section 55 concerns the wilful obtaining, disclosing or procuring of information without the data controller's consent. The prohibitions in this section apply equally to everyone. The defences listed in section 55(2) apply to everyone and include section 55(2)(d) which requires the knowing or reckless obtaining,

disclosing, or procuring information without the consent of the data controller to be justified in the public interest.

The purposes of the provisions are very different. Section 32 ensures that the data protection principles do not prevent responsible journalism; whilst the defence to section 55 ensures that the prohibition on the misuse of personal data does not prevent disclosures which are in the public interest.

During the parliamentary debates for the Data Protection Bill, Mr George Howarth, the then Parliamentary Under-Secretary of State for the Home Department explained the difference between the sections. He said, "it is not sufficient that the obtaining, disclosing or procuring should be in the public interest; it must also be justified as being in the public interest in all the circumstances of a particular case. That makes the threshold for the test being satisfied a little higher than the simple public interest test ...We have included [the word justified] to help to narrow the scope of the provision, to limit reliance on the exemption to cases in which there is a genuine justification for what is being done."[18]

The Government does not agree that it is necessary to amend section 55 to extend the exemption in section 32. We are not proposing to criminalise any conduct that is not currently against the law. The section 55 offence - with its public interest defence and other defences - is a proportionate measure to deal with the risks to people's privacy that have been identified. Therefore there is no need to widen the defence to reconcile privacy and freedom of expression.

The British Computer Society stated that unless the courts are willing to impose the maximum sentence, the revisions to the Act will have no effect and it is unlikely that guidelines will assist in this respect.

The Government's response: Courts are required to impose sentences that are commensurate with the seriousness of the offence, following consideration of the facts and whether a custodial, community or other sentence is the most appropriate. The formulation/ introduction of sentencing guidelines will also help to ensure a consistent sentencing policy and that available sanctions are applied effectively. The maximum sentence will be imposed as appropriate and in accordance with the sentencing principles.

The Council of Circuit Judges was generally supportive of the proposals. However, they expressed reservations about the issuing of formal guidelines, it was argued

---

[18] House of Commons, Standing Committee D. 2 June 1998.

that there was a need for flexibility in sentencing to take account of the almost infinite variety of circumstances that can arise. They added, "as we have pointed out in response to other consultations no matter how a guideline is framed it tends to be perceived as rigid."

In contrast DfES argued that guidelines were not drawn up without consultation; they stated that guidelines are informed by advice from the SAP, which is staffed by senior lawyers and members of the judiciary, and are subject to revision.

Additional comments

In addition to providing a response to the questions a number of respondents made recommendations or asked the Department to consider certain issues. These are discussed below.

Guidance

A number of respondents were in favour of introducing guidance. The Law Society of Scotland stated that clear guidance on the law may prevent unintentional disclosure and should include examples of when the offence may be committed in different circumstances and when the offence has not been committed. Privacy Laws & Business requested that the ICO's office should issue guidance on how it intends to exercise its prosecution powers and include similar examples with possible penalties. They added that it would be useful if it could indicate circumstances where the ICO would consider pursuing corporate/ board level responsibility for an offence.

DfES also recommended clear guidance to practitioners on when they may legally share personal data. DfES published the first cross Government guidance for practitioners in children's services sharing information on children and young people on 6 April 2006.

CIFAS argued that the introduction of sentences could have the undesirable effect of hampering legitimate data sharing. They emphasised the importance of detailed guidelines for any new regime, which should include safeguards to protect those who disclose in good faith.

The ICO has given a commitment that any legislative changes will be supported by further guidance.

Negligent disclosure

In response to question 1, HMRC stated that the Commissioners for Revenue & Customs Act 2005 (CRCA) which creates an offence for the wrongful disclosure of information about a person, has no requirement to prove the 'wilful abuse' of data for the breach to occur. Under this Act, negligent disclosure is therefore an offence. The Act also applies to information about both natural and legal persons. It was suggested that DCA amend the criteria for committing an offence in the DPA, to result in a consistent approach and help align legislation.

The CRCA criminal offence against wrongful disclosure protects all of the information about, acquired as a result of, or held in connection with the exercise of HM Revenue and Custom's functions. This covers information about its customers including personal and business data. Personal data held within HMRC is currently protected by the CRCA criminal offence. In contrast the DPA refers to a broader category of personal information by protecting personal data wherever it is held. The Government does not wish to amend the DPA to make negligent disclosure an offence under the DPA. Both criminal offences ensure that those members of staff (both public and private sector) who act in the reasonable belief that they are entitled to disclose the information will not be guilty of an offence. Under the DPA those who are duped into giving information should not be prosecuted.

initiatives to increase data sharing

A number of respondents including the Council of Circuit Judges remarked that some people might express reservations at the notion of greater data sharing within the public sector in light of increasing concerns regarding identity theft, which is often facilitated by the unauthorised disclosure of confidential information. They added that any loss of privacy rights should be proportionate to the perceived benefit.

Privacy Laws and Business stated that despite initiatives to facilitate appropriate information sharing – which are running in parallel with the proposal for tougher penalties – there was a risk that the increased penalties would lead to a reduction in legitimate data sharing/ flows. They argued that proper consensus on the nature and extent of this data sharing (e.g. by way of a DS Bill) would mitigate this risk. They added that organisations might be reluctant to share data if they feared that they or their members of staff could be prosecuted as a result.

For this reason, a number of respondents welcomed the confirmation that those who made an error of judgement would not be penalised. One respondent said that this message should be reinforced in legislation and/ or publicly issued by the ICO or DCA.

The Government is committed to more information sharing between public sector organisations and service providers. We recognise that the more we share information, the more important it is that people are confident that their personal data is kept safe and secure. Increasing the public confidence in the sharing of personal data is one of the aims of the Government's wider strategy on data sharing. The Government is strongly committed to the protection and security of personal data.

The "*Information sharing vision statement*"[19] set out the Government's vision for better, more customer focused services supported by greater information sharing which will protect and support individuals and society as a whole:

"There are enormous benefits to sharing information....We must, of course, properly use the provisions in the Data Protection Act as a safeguard to protect privacy and confidentiality but it must not be used to justify unnecessary barriers to sharing information. Our vision is to ensure that information will be shared to expand opportunities for the most disadvantaged, fight crime and provide better public services for citizens and business, and in other instances where it is in the public interest."[20]

The benefits to increased information sharing – as discussed in the vision statement – include improving opportunities for the most disadvantaged, reducing crime, reducing the burden on business, more effective and targeted customer focused public services and policy implementation.

Section 55 does not apply to those who act in the reasonable belief that they had the right in law to obtain or disclose information or that they would have had the consent of the data controller. It does apply to those who abuse the trust placed in them by their employers, or those who cajole information from organisations. Section 55(2) lists the exceptions. As mentioned earlier, any changes to the legislation will be supported by guidance issued by the ICO.

Difficulties in obtaining information

The FLA was concerned that some breaches of the Act might be caused by the difficulty sometimes faced by organisations in obtaining information about debtors for legitimate reasons, and faced by private investigators when investigating criminal cases. They asked the DCA to give some consideration to ways of overcoming this.

If a creditor requires personal data in order to enforce a debt, or a private investigator needs information to investigate a case of fraud, then the people who hold the information may disclose it in accordance with s35 of the DPA. This section disapplies certain requirements of the DPA in order to facilitate the disclosure of data. It applies where the disclosure of information is required by law

---

[19] DCA 47/06 HM Government: Information sharing vision statement 13 September 2006 http://www.dca.gov.uk/foi/sharing/information-sharing.pdf
[20] As above, P5.

or made in connection with any legal proceedings (including prospective proceedings), for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights. If the data controller is not willing to disclose the information, then a court order can be sought as appropriate.

Public and private sector

CIFAS also felt that there was an unfortunate emphasis on the public sector in parts of the consultation paper, and this might raise questions in the mind of respondents as to the application of the proposals to the private sector.

The Government's proposals would apply to anyone that handles personal information placed under legal obligations by the Data Protection Act 1998, whether they work in the private or the public sector.

It might also help to clarify that the following statement applies to both those in the private and public sector: We want to make it absolutely clear that this does not mean penalising [people] who, while sharing data for legitimate reasons, make an error of judgement in what are often marginal and complex cases. For instance, where a [person] who shares data in order to protect a child, doing so in the reasonable belief that they have the right in law and having made the judgement that it is necessary to do so, subsequently finds out that the information should not have been shared, will **not** be guilty of an offence under section 55. Likewise a staff member who is deceived into giving out information will not be guilty of an offence.[21]

Consent

Transport for London (TfL) encouraged DCA to consider amending s55 to address situations where the data controller's consent had been given but obtained by deception, because it would avoid arguments regarding the validity of the data controller's consent.

This suggestion goes beyond the scope of the proposals because consent is referred to in various places within the DPA. Any amendment to the definition of consent might affect the interpretation of consent elsewhere in the Act, which is not our intention.

---

[21] Increasing penalties for deliberate and wilful misuse of personal data. P3.

Comments on the Partial Regulatory Impact Assessment

The Consultation Paper welcomed comments on the Partial Regulatory Impact Assessment (RIA).

There were only two comments.

The European Information Society Group (EURIM) believes that the Partial RIA seriously understated the benefits.

The Information Commissioner, Richard Thomas made a comment in respect of the following sentence "the Government does not however, consider the creation of a new custodial sanction will increase the number of prosecutions brought forward by the prosecuting authorities."[22]

He stated that whilst it is unlikely that the ICO will bring a significantly higher number of cases, it is appropriate to note that the Director of Public Prosecutions also has the power to bring prosecutions under the DPA. He added that on some occasions the police and Crown Prosecution Service choose not to bring prosecutions under the Act and use other legislation, which carries custodial sentences instead, despite the fact that the section 55 offence better fits the circumstances of the crime.

He said that whilst the number of prosecutions are likely to increase, there is likely to be a corresponding decline in prosecutions under other legislation. Therefore he anticipates the impact on costs to be neutral.

In light of these comments and the overall response to the consultation, the Government will proceed with Option 2 as described in the Partial RIA. The Partial RIA will be updated accordingly and will be available on our website.

---

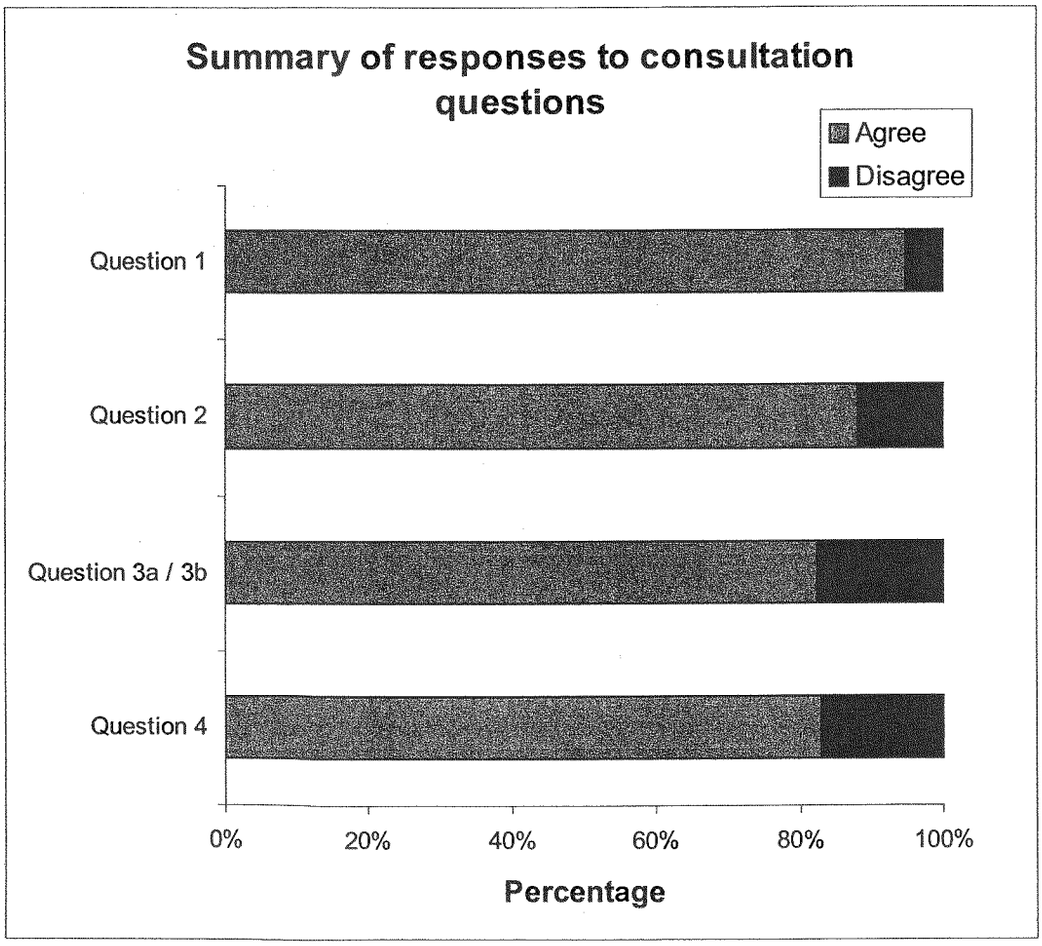
[22] Increasing penalties for deliberate and wilful misuse of personal data. P23.

Conclusion and Next Steps

The proposal to introduce custodial penalties as an option available to the courts when sentencing those found guilty of offences under section 55 of the DPA, was generally welcomed by respondents. The percentage of respondents who agreed with the proposal is shown in the graph below.

Figure 6: Summary of responses to consultation questions

Percentage of respondents who agreed and disagreed with each question.



The Government is therefore minded to amend section 60 of the Data Protection Act 1998 to allow for, in addition to the current fines:

- On summary conviction, up to six months imprisonment (which will be increased to twelve months imprisonment in England and Wales when s154 of the Criminal Justice Act 2003 comes in to force and in Scotland when s35 of the Criminal Proceedings etc. (Reform) (Scotland) Act 2007 comes into force);); and

- On conviction on indictment, up to two years imprisonment.

The Government believes that the introduction of custodial penalties will be an **effective deterrent** to those who seek to procure or wilfully abuse personal data, as agreed by the majority of respondents. It is clear that current financial sanctions are not solely a sufficient deterrent to those engaged in the illegal trade in personal information.

The suggested **sentence lengths** (as above) are appropriate, and commensurate with the seriousness of the offence. It is crucial that there is consistency across all pieces of legislation, which deal with offences of this nature. The DPA as the central piece of legislation, which governs the processing of personal data and applies to both the public and private sector, should be amended to allow for comparable sanctions.

The Sentencing Guidelines Council will issue **guidelines** for the offence as appropriate, following advice from the Sentencing Advisory Panel and public consultation.

The Government will seek to introduce **legislation** as soon as parliamentary time allows.

We have considered the human rights issues, which include proportionality and compatibility. The ICO's report *"What Price Privacy? The unlawful trade in confidential personal information"* underlined the extent of non-compliance with section 55 of the DPA and provided evidence that the existing penalties are not sufficiently protecting the rights of individuals, notably the right to a private and family life (Article 8). The Government concludes that the increased penalties are necessary to protect people's rights and any interference with journalists' freedom of expression (Article 10) would be justified and proportionate. The proposal is therefore compatible with the European Convention on Human Rights.

The Government is committed to more information sharing between public sector organisations and service providers, to enable more customer focused services

supported by greater information sharing which will protect and support individuals and society as a whole.

The Government has an excellent track record of strengthening individuals' rights to privacy and the legislative framework, provided by the Data Protection and Human Rights Acts, will continue to offer a robust statutory framework to maintain those rights whilst sharing information to deliver better services.

Consultation Co-ordinator contact details

If you have any complaints or comments about the **consultation process** rather than about the topic covered by this paper, you should contact the Department for Constitutional Affairs Consultation Co-ordinator, Laurence Fiddler, on 020 7210 2622 or email him at consultation@dca.gsi.gov.uk

Alternatively, you may wish to write to the address below:

Laurence Fiddler
Consultation Co-ordinator
Department for Constitutional Affairs
5th Floor Selborne House
54-60 Victoria Street
London
SW1E 6QW

If your complaints or comments refer to the topic covered by this paper rather than the consultation process, please direct them to the contact given on page 3.

The Consultation Criteria

The six consultation criteria are as follows:

1. Consult widely throughout the process, allowing a minimum of 12 weeks for written consultation at least once during the development of the policy.

2. Be clear about what your proposals are, who may be affected, what questions are being asked and the timescale for responses.

3. Ensure that your consultation is clear, concise and widely accessible.

4. Give feedback regarding the responses received and how the consultation process influenced the policy.

5. Monitor your department's effectiveness at consultation, including through the use of a designated consultation co-ordinator.

6. Ensure your consultation follows better regulation best practice, including carrying out a Regulatory Impact Assessment if appropriate.

These criteria must be reproduced within all consultation documents.

Annex A – List of Respondents

We are grateful to all the stakeholders who responded to this consultation. Responses were received from:

1. ACXIOM
2. AEGON UK
3. Peter Allen
4. APACS
5. Association of British Insurers [ABI]
6. Association of Chief Police Officers [ACPO]
7. Bisnode PLC
8. British Bankers Association [BBA]
9. British Computer Society [BCS]
10. British Medical Association [BMA]
11. Christchurch Borough Council/ Dorset Information Management and Compliance Working Group
12. CIFAS
13. Confidential response
14. Council of HM Circuit Judges
15. Alan Cox
16. Crown Prosecution Service [CPS]
17. Data (Practical Application) Protection Ltd

18. Department for Education and Skills [DfES]
19. Department for Transport [DfT]
20. The Direct Marketing Association [DMA]
21. Michael Doherty
22. Environment Agency
23. Equifax
24. Ernst & Young LLP
25. European Information Society Group [EURIM]
26. Experian
27. Faculty of Advocates
28. The Finance & Leasing Association [FLA]
29. Financial Services Authority [FSA]
30. Friends Provident
31. The General Medical Council [GMC]
32. Grampian Health Board
33. Greater Manchester Health & Social Care Information Governance Local Learning Group
34. Greenwich Council
35. Guardian News & Media [GN&M]
36. Health and Safety Executive [HSE]
37. HM Revenue & Customs [HMRC]
38. The Information Commissioner's Office [ICO]

Increasing penalties for deliberate and wilful misuse of personal data
Summary of responses

39. Institute for the Management of Information Systems [IMIS]

40. The Law Society of Scotland (Privacy Law Sub Committee)

41. Leicester Partners NHS

42. The Magistrates' Association: Judicial Policy & Practice Committee

43. Market Research Society [MRS]

44. Ministry of Defence [MoD]

45. National Archives of Scotland

46. National Health Service [NHS]

47. Nationwide

48. Newspaper Publishing Association,

    Newspaper Society

    Periodical Publishers Association

    Scottish Newspaper Publishers Association

    Society of Editors

49. Office of Communications [Ofcom]

50. Office of Fair Trading [OFT]

51. Ofgem

52. Peterborough City Council

53. Privacy Laws & Business (Anonymous Client)

54. Privacy Laws & Business

55. The Royal Academy Of Engineering

56. Scottish Ambulance Service

Increasing penalties for deliberate and wilful misuse of personal data
Summary of responses

57. The Security Institute [SI]

58. Serious Fraud Office [SFO]

59. Socitm Consulting

60. South Holland District Council

61. Staffordshire Moorland District Council

62. Transport for London [TfL]

63. Wrightington, Wigan & Leigh NHS Trust

Produced by DCA
7 February 2007
CP(R) 9/06