Fraud Advisory Panel

Perceptions on the impact of data protection legislation on the successful private sector investigation of fraud

A Preliminary Study

First published 2006

Fraud Advisory Panel

Perceptions on the impact of data protection legislation on the successful private sector investigation of fraud

A Preliminary Study

March 2006

Professor Martin Gill

Douglas S Smith MSc MIRM

Martin Hemming MSc LLB

Research conducted by

Perpetuity Research and Consultancy International (PRCI) Ltd

Sponsors

Founded in 1988, CIFAS – the UK's Fraud Prevention Service, is a not-for-profit membership association dedicated to the prevention of financial crime. CIFAS provides a range of fraud prevention services to its Members, including a fraud avoidance system used by the majority of the UK's financial services companies. CIFAS also represents its Members to government, the media and the business community, and provides best practice guidance, training and networking opportunities. CIFAS services are offered to the general public through its Protective Registration Service which helps to protect consumers from identity fraud. Today the CIFAS membership encompasses consumer credit, telecommunications, factoring, insurance, utilities, share dealing and commercial credit. There are over 240 companies in membership and in 2005 CIFAS Members reported saving £682 million as a result of sharing data with one another through the CIFAS system. **www.cifas.org.uk**

The Telecommunications United Kingdom Fraud Forum (TUFF) is a United Kingdom based Forum which provides an environment where members can exchange information and knowledge as it relates to the detection and prevention of fraud and crime within the telecommunications industry. Membership is open to companies whose core business is provision of telecommunications or telecommunications-related (including equipment manufacturers) services. Current membership is representative of a wide spectrum of mobile, fixed and indirect access companies and significant service providers from the UK telecoms industry. **www.tuff.co.uk**

The Law Society is the regulatory and representative body for 116,000 solicitors in England and Wales. We *regulate* and set standards for solicitors to make sure they deliver a good and ethical service to consumers. We *support* solicitors to help them achieve the standards expected of them, and deliver good service. We *represent* solicitors and we *influence law reform* to achieve a better system of justice. **www.lawsociety.org.uk**

The Association of Chartered Certified Accountants (ACCA) is the largest and fastest-growing international accountancy body. Over 320,000 students and members in 160 countries are served by more than 70 staffed offices and other centres. ACCA's mission is to work in the public interest to provide quality professional opportunities to people of ability and application, to promote the highest ethical and governance standards and to be a leader in the development of the accountancy profession. ACCA is pleased to support the important work of the Fraud Advisory Panel and in particular to support this research project which looks into an area of growing legal and technical significance for the successful fight against fraud. **www.acca.org.uk**

The Centre for Business Performance promotes and funds, through the ICAEW's charitable trusts, leading-edge research on performance-related issues of immediate and long-term importance to the business community. The aim is to promote high-quality research of interest to the accountancy profession and the wider business community. The views expressed in this publication are those of the authors and are not necessary those of the Centre for Business Performance nor of the Institute of Chartered Accountants in England and Wales. **www.icaew.co.uk/centre**

Contents

Foreword

Fraud directed against business in the UK is growing at an alarming rate and the requirement placed on the private sector to do as much as it can to prevent fraud from happening is being recognised. Firms are putting in place more effective controls to identify and manage the risk of fraud. But where fraud occurs, as it inevitably will, despite the most rigorous safeguards and because of competing demands on law enforcement, the private sector must increasingly rely on its own resources to put an investigation in motion. Forensic accountants and private-sector detective and investigation agencies have never been as much in demand as now and that demand is increasing. At the same time, companies and business, whether on their own or through trade associations, are exploring every possible avenue to prevent and deter fraud. One of the most obvious approaches is to share data relating to fraud between businesses and across sectors. Much fraud against business is now professionally organised; patterns of deceptive and dishonest behaviour can be identified which are replicated across business sectors by gangs who do not discriminate as far as their victims are concerned. It is vital for effective defence against the threat of fraud that businesses can see what has happened elsewhere and recognise the pattern. They can do this only if a firm which has been targeted by fraudsters is willing and able to exchange details with others who might become future victims. Equally, the public sector holds information which could be of vital importance to firms to verify employment records of potential staff members, to check credit claims and to avoid becoming the victims of identity fraud.

At the same time, it must be recognised that there is a very real need to protect personal details about individuals and ensure that disclosure made by organisations that hold personal information is done only for necessary and requisite purposes. The legislation which is in place to ensure that that happens mirrors the European requirements and is overseen by the Information Commissioner's Office. The machinery to enforce the legislation should, in theory, safeguard our liberties while at the same time enabling those who need it to have proper access to personal information for the purpose of presenting and investigating crime. In practice, this does not appear to be happening with the ease and readiness of access that should be expected. Why is this? The Information Commissioner's Office itself notes that "Some organisations understandably err on the side of caution and do not release information when they could do so. Unfortunately, some organisations continue to use the Data Protection Act 1998 as an excuse not to do something, rather than seeing it as good business sense to treat their customers and their information with respect." And, one could add, to assist each other in preventing and deterring fraud.

The Fraud Advisory Panel commissioned this initial research to try to discover what barriers business and professional advisers identified as preventing data sharing for the purpose of investigating and preventing fraud and what their perceptions were of how the legislation was working in practice. The pilot study, which we publish here, uncovers some worrying perceptions of the legislation and its effects. The study demonstrates that there are some real problems in this area which are hampering investigations and allowing fraud to spread unchecked across organisations and sectors when, with the better communication of information permitted by the legislation, much fraud could be stopped in its tracks, or at the very least, effectively investigated.

We would like to acknowledge the invaluable support of our sponsors, CIFAS – the UK's Fraud Prevention Service, the Association of Chartered Certified Accountants (ACCA), the Law Society of England and Wales, and the Telecommunications United Kingdom Fraud Forum (TUFF), and the support and assistance received from Institute of Chartered Accountants in England and Wales (ICAEW) staff, in particular the Centre for Business Performance. The Fraud Advisory Panel would also like to thank Felicity Banks, Chris Brogan, Mia Campbell, Neil Griffiths, Mary Sambrook and Ben Summers for their invaluable support, comments and input.

Rosalind Wright CB
Chairman

March 2006

Executive summary

- This report describes a small-scale preliminary study designed to assess how and to what extent data protection legislation impacts on private-sector fraud investigation.

- Twenty-two subjects were interviewed, representing 15 undertakings and covering a range of companies including banks and building societies, insurance companies, organisations involved in fraud advice and investigation, a credit reference agency, a firm of solicitors and a firm of accountants.

- Almost all those interviewed considered a lack of proper understanding of the provisions of the Data Protection Act 1998 (DPA 1998) was leading to a presumption in favour of non-disclosure of data and a consequent compromising effect on private-sector investigations of allegations of fraud.

- There was a perception of a lack of clarity in the provisions of the Act itself. A lack of judicial authority in this area further exacerbated the problem. Data controllers were perceived to be 'hiding behind the Act' to justify their non-cooperation in private-sector fraud investigations. Participants suggested that more guidance on the application of the Act would be helpful.

- Those organisations that appeared to have good procedures and policies in place tended to have fewer problems with fraud investigation or obtaining information. These organisations had forms and procedures for a wide range of eventualities.

- The better a fraud investigation team was at building internal and external relationships, the better results it achieved in acquiring data.

- Trust plays an important role in the release of data. Trust gives organisations confidence to release data to other parties.

Recommendations

This study has identified scope for further in-depth research in this area. This might include a more extensive study of the type outlined in this report, to include the perspectives of the police, the Information Commissioner's Office (ICO) and a wider range of financial institutions and investigators.

In addition, the study recommends that:

- The ICO should consider the provision of additional practical guidelines, with scenarios of good and bad practice, to inform the investigative process.

- Data relating to deceased persons should be made available, subject to adequate safeguards to ensure it is passed only to appropriate persons or bodies; at the very least, it should be easier for legitimate investigators to obtain.

- Data relating to passports and driving licences should be made available, subject to adequate safeguards to ensure it is passed only to appropriate persons or bodies; at the very least, it should be easier for legitimate investigators to obtain.

- There is an urgent need for investigators to be trained in data protection legislation and case law.

- The Security Industry Authority (SIA) needs to apply stringent licensing requirements to investigators, both private and in-house, where these are not already subject to effective professional or regulatory oversight.

- A joint working group should be established to develop best practice guidelines for the exchange of information between financial institutions and private investigators.

- An effective trade or representational group for private investigators could assist in the provision of appropriate guidance, manage relationships with other organisational groups such as the banks, and lobby for changes in the legislation, where desirable.

Introduction

Aims of this research

This report describes a small-scale preliminary study which aimed to assess how, and to what extent, data protection legislation affects the conduct of private-sector investigations into private-sector fraud in the UK, and in particular whether the legislation makes successful investigations easier or more difficult to accomplish. There are three main issues raised by the research question, and these provide the rationale for the methodology, which is detailed fully in a later section.

1. What does data protection legislation set out to accomplish, and how have its provisions been changed by successive Acts of Parliament and by decisions of the courts in landmark cases?

2. How has the legislation been interpreted by those most affected, in particular the police and other institutions which collect personal data and control its disclosure?

3. How do victims and potential victims who commission investigations (the 'customers'), and those who conduct investigations (the 'suppliers') define and measure success, and do they view the impact of data protection legislation as positive or negative?

Background: a brief review of legislation and interpretation[1]

The history of data protection legislation in the UK began with the enactment of the Data Protection Act 1984 (DPA 1984), which legislated for the appropriate control of electronically stored personal data. DPA 1984 was concerned only with data stored electronically, and left in place opportunities for investigators to legally gather confidential personal information on individuals if it was processed manually. For this reason, and to give effect in UK law to the 1995 European Community (now European Union) 'Directive on The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data', DPA 1984 was repealed and superseded by the Data Protection Act 1998 (DPA 1998). While this, together with the Human Rights Act 1998 (HRA 1998), may help prevent possible malpractice by investigators, it is possible that in so doing it may have created opportunities for offenders to conceal their wrongdoing behind a veil of legally enforced privacy. Put simply, investigators and victims of some forms of crime claim that data protection legislation is impeding investigation and the pursuit of justice.

[1] This short review of the literature and decided cases is presented to give an indication of legal issues that might arise in investigations. Nothing in this report should be taken as a formal legal opinion on the current state of the law.

The balance between an individual's right to privacy and society's right to ensure that wrongdoers cannot avoid detection and prosecution is, and always has been, a fine one. New legislation often results in claim and counter-claim from law enforcers and civil liberties groups that the balance has been tilted too much one way or the other. For example, the Police and Criminal Evidence Act 1984 (PACE 1984) imposed a raft of new restrictions on police officers which, it was anticipated, would hinder the investigation of crime. However, experience of compliance with PACE 1984 revealed distinct advantages for investigators, such as the specification of clear guidelines that simplified cases and helped codify professional standards and practice. New legislation may therefore pose a temporary challenge rather than rendering investigators at a permanent disadvantage before the law.

In the context of this project, the term 'successful investigation' is worthy of exploration. By one definition it can refer to an investigation that leads to a conviction. However, prosecutions are costly and time-consuming, can attract unwanted publicity and may also damage staff morale. A 'successful' investigation may, therefore, also include identifying the culprits and applying internal disciplinary measures, justifying dismissal, securing their resignation, facilitating a civil action or simply informing revision of security policy and procedures. This suggests a need to accommodate informal means of identifying fraud and punishing it, as well as formal criminal prosecutions. Any legislation that deters victims from seeking redress from fraudsters is also undesirable.

The DPA 1998, together with a number of associated Statutory Instruments, came into force on 1 March 2000. One of its purposes is to protect individuals' personal data (see Annex B for a definition of this term). Newman[2] typified private investigation practitioners' reaction to the DPA 1998 when he wrote:

> *The emphasis has always been on the individual's rights. It goes no way to addressing the rights of the general populace who may be affected by the ability of certain parties to avoid detection by virtue of the legislation.*

In fraud investigation personal data may be required by investigators, and Newman's argument is that the DPA 1998 hinders the ability to investigate frauds. To maximise success, fraud investigators generally need to acquire and match data quickly, and the perception exists that by delaying or preventing data acquisition the DPA 1998 disadvantages the investigator. There is also a perception that other legislation which reinforces personal rights compounds these problems.

[2] Newman, R. (2003) *Data Protection: A Best Practice Guide for Professional Investigators* UK: Association of British Investigators.

The DPA 1998 was designed to give effect to European law, and one important consequence of this was explicitly referred to by the Master of the Rolls, Lord Phillips of Worth Matravers, in his judgement in the landmark case *Campbell v Mirror Group Newspapers in 2002*:

> *In interpreting the Act it is appropriate to look to the Directive for assistance. The Act should, if possible, be interpreted in a manner that is consistent with the Directive. Furthermore, because the Act has, in large measure, adopted the wording of the Directive, it is not appropriate to look for the precision in the use of language that is usually to be expected from the parliamentary draftsman. A purposive approach to making sense of the provisions is called for.*[3]

What this means is that those interpreting the DPA 1998 must not restrict their interpretation to the actual words used in the statute, but rather interpret those words in such a way as to take proper account of the purposes for which it was passed:

> *...notably the right [of individuals] to privacy and accuracy of their personal data held by others ('data controllers') in computerised form or similarly organised manual filing systems...*[4]

Some might infer from this that the privacy of individuals takes precedence over other considerations, such as the need to bring wrongdoers to justice, although the DPA 1998 does allow disclosure of personal data in defined circumstances connected with law enforcement. Section 29 provides that personal data may be processed (which includes disclosure) for any of the following purposes:

a) the prevention or detection of crime

b) the apprehension or prosecution of offenders

Furthermore, Section 35 (2) provides that:

> *Personal data are exempt from the non-disclosure provisions where the disclosure is necessary –*
>
> *(a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or*
>
> *(b) for the purpose of obtaining legal advice, or*
>
> *(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.*

These provisions appear to allow disclosure of personal data to such interested parties as victims of crime and those acting on their behalf, such as private investigators, although

---

[3] [2002] EWCA (Civ) 1373.

[4] Lord Justice Auld in *Durant v Financial Services Authority (FSA)* [2003] EWCA (Civ) 1746.

a pre-condition for legitimate processing under Schedule 2 (or Schedule 3 in the case of sensitive data) would still have to be established. Even in those circumstances, it is possible that difficulties might still be experienced with data controllers who require proof that a request for disclosure from somebody other than a police officer is actually for the stated purpose. In any event, data controllers may not be aware of the disclosure gateways that exist, or may deny such awareness, and as a result still refuse to disclose unless ordered by a court to do so. This would have the effect of delaying disclosure to the point where an investigation is prejudiced.

The *Durant* case (*Durant v FSA*)[5] was a landmark case decided by the Court of Appeal. The case concerned Mr Durant's right to obtain disclosure of documents created by the FSA in response to a complaint he made about the conduct of Barclays Bank.

Two main arguments were considered by the Court of Appeal: the first related to the definition of 'personal data' within the meaning of the DPA 1998. Counsel for Mr Durant submitted that a broad definition of what constitutes 'personal data' should be applied. On this broad definition, the FSA would have to disclose:

> *any information retrieved as a result of a search under [Mr Durant's] name, anything on file which had his name on it or from which he could be identified or from which it was possible to discern a connection with him.*

Counsel for the Bank contended for a narrower definition.

The Court concluded that:

> *... mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data. Whether it does so in any particular instance depends on where it falls in a continuum of relevance or proximity to the data subject as distinct, say, from transactions or matters in which he may have been involved to a greater or lesser degree.*

The Court of Appeal decided that a narrow definition of personal data was to be applied, and that 'the mere fact that a document is retrievable by reference to [a data subject's] name does not entitle him to a copy of it under the Act'.

Secondly, the Court of Appeal was asked to clarify what constituted a 'relevant filing system' whose contents, along with electronic systems, come within the meaning of 'data' and thus fell within the regime established by the DPA 1998. The finding of the Court was that:

---

[5] Ibid.

It is plain from the constituents of the definition considered individually and together, and from the preface in it to them, "although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose", that Parliament intended to apply the Act to manual records only if they are of sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system. That requires a filing system so referenced or indexed that it enables the data controller's employee responsible to identify at the outset of his search with reasonable certainty and speed the file or files in which the specific data relating to the person requesting the information is located and to locate the relevant information about him within the file or files, without having to make a manual search of them. To leave it to the searcher to leaf through files, possibly at great length and cost, and fruitlessly, to see whether it or they contain information relating to the person requesting information and whether that information is data within the Act bears ... no resemblance to a computerised search. It cannot have been intended by Parliament – and a filing system necessitating it cannot be "a relevant filing system" within the Act. The statutory scheme for the provision of information by a data controller can only operate with proportionality and as a matter of common-sense where those who are required to respond to requests for information have a filing system that enables them to identify in advance of searching individual files whether or not it is "a relevant filing system" for the purpose.

It may be that this definition of a 'relevant filing system' assists investigators who seek disclosure of, or who themselves maintain, data in manual form where searching cannot readily be conducted in that the judgement narrows the definition of 'relevant filing system' so that fewer manual records are now covered by the Act than had previously been thought. A data protection objection to disclosure can no longer be raised in relation to manual records which fall outside the Court of Appeal's expanded definition. The reasoning in *Durant* has since been followed in a subsequent case, *Smith v TSB*.[6]

The Freedom of Information Act 2000 (FOI 2000), which came fully into force in January 2005, has now extended the definition of 'data' to include any paper-based personal information recorded by a public authority, irrespective of the structure of the filing system. This will have implications for a number of public authorities, including the FSA, which is now a member of the public sector.

Of course, in many circumstances in which an investigator makes a request for information, there may be other 'non-Data Protection Act' legal considerations which would prevent a disclosure. For example, the information may be subject to a duty of confidentiality or legal professional privilege. However, this report is confined to examining the effect of data protection legislation on investigators and does not purport to examine the other legal barriers which may stand in the way of disclosures to investigators.

[6] [2005] EWHC 246 (Ch.).

Methodology

This was a preliminary study to identify the issues and concerns held by professionals working with data protection legislation in the private sector, and to gather their views on the impact of the legislation on private-sector fraud investigation. The research was undertaken between November 2004 and February 2005.

The project began with a period of desk research to assimilate details of the legislation and identify key issues. Semi-structured interviews were then conducted with 15 subject organisations (a copy of the interview schedule can be found at Annex A), four by telephone and 11 face-to-face, between 23 November and 17 December 2004.

The semi-structured interview is adept at eliciting participants' views on a range of key issues that have been defined in preparatory work, while leaving scope to explore interesting issues in depth.

Participants received a copy of the questions in advance of the interview, to give them time to consider their responses. The participants came from a range of companies across the UK, including financial institutions (retail banks, building societies, insurance companies and a merchant bank), a credit reference company, a major fraud advisory service, an investigators' association, a data-mining company and forensic accounting firms. The occupations of people interviewed included fraud investigators, forensic accountants, company directors, private investigators and lawyers. The 15 interviews actually represent the views of 22 individuals, because in some interviews both the data handler[7] and the practitioner employed by the same organisation were present.

Although the number of people interviewed was small, it is worth noting that the interviews were comprehensive and provided ample opportunity to explore all relevant issues affecting data controllers and investigators in relation to the DPA 1998. However, the small sample size restricted the conclusions that could be drawn.

The findings explore the issues that practitioners face in controlling data and investigating private-sector fraud and whether the DPA 1998, helps, hinders or has no effect on their investigations.

Definitions of terms can be found in Annex B.

[7] 'Data handler' is a general term used to describe a person or entity that might come into contact with data, including data processors and data controllers. This term is used to avoid confusion with the definitions of data processor and data controller in the DPA 1998.

Findings

This section presents the findings from the interviews with practitioners and data handlers. Except where indicated, opinions in this section are views expressed by interviewees, and where conflicting views were expressed an appropriate balance has been attempted. Generally the presentation follows the structure of the interview schedule (Annex A), but it also includes certain other themes which emerged and which either attracted wide consensus or were raised by several participants, and these are given due prominence.

The views gathered and summarised in this section are the result of the research team raising specific issues and inviting comment.

The investigation process

The interviews considered the context of the investigation process. All participants agreed that the main elements of an investigation were:

- a precipitating event;
- an initial risk assessment;
- a decision to conduct a preliminary review;
- data-gathering;
- a decision to conduct, or not to conduct, a full investigation; and
- an outcome.

Participants noted that most of the problems encountered that could be attributed to the DPA 1998 were associated with the first four elements of the investigation.

This is because it is not clear until a preliminary review and some initial data gathering have been completed that there is anything substantive to investigate.

Definition of 'personal data'

Most participants claimed that they understood the definitions of personal data in DPA 1998, but that problems arose when trying to interpret definitions containing words such as 'reasonable', 'public good' and 'proportional'. As one participant put it, 'there is a distinct lack of clear definitions'. Difficulty has been encountered recently with the interpretation of the word 'reasonable' in other circumstances (e.g. 'reasonable force' to prevent burglary). Participants mentioned that one person's view of 'reasonable' can be quite different to another's.

Others claimed that although they understood the definition of personal data, many people that they requested information from did not. For example, one investigator reported that she had requested information from a public body about a dead person, and was told that this could not be disclosed because it would contravene DPA 1998, despite the fact that personal data is defined in Section 1 of the Act as 'data which relate to a living individual'. The ICO's legal guidance document, section 2.2.2, also makes the position clear.[8] Access to deceased persons' data can be critical in fraud prevention, particularly if it is suspected that their identities have been stolen for dishonest purposes.[9]

Problems were also reported with data controllers using DPA 1998 as an excuse not to disclose data that could be considered public. A common view expressed by participants was that it was not the DPA 1998 itself that was blocking proper fraud investigation, but rather individual data handlers who were interpreting its provisions incorrectly.

Other types of data that were considered important in fraud investigation but are not currently available are driving licence and passport information. However, statute restricts access to these types of information.

Lack of sharing through misunderstanding

Almost all of those interviewed considered that lack of proper understanding of DPA 1998's provisions was leading to fear of litigation amongst data handlers. In the view of many participants this had been exacerbated by a lack of rigorous testing of the Act in the courts, which has led to divergent opinions of the law, especially amongst lawyers. This in turn had reportedly led to paralysis and a presumption in favour of non-disclosure, with DPA 1998's definition of what constitutes non-disclosable personal data and relevant filing systems being given a wide definition. Many participants were unfamiliar with the *Durant* case, but some of those who knew the details felt the judgement would be reversed in due course. Only one participant felt that the judgement had made a useful contribution to defining the terms of DPA 1998.

One participant stated that 'the willingness to put personal data into an electronic database is undermined, yet the power of such databases is essential to fraud investigations'.

During the first four phases of an investigation as described above, some participants managed this conflict by creating rudimentary manual files which, following the *Durant* case, they considered might not be regarded as personal data and would therefore not need to be disclosed to subjects.

[8] Information Commissioner's Office (2004) *Data Protection Act 1998, Legal Guidance, Version 1*.
[9] Of course, some information on deceased persons is publicly available: for example, probate registers.

Data covered by the Act

The view of the ICO on the types of data that might be included within DPA 1998's definition of personal data is wide-ranging. Participants indicated that in some situations it was obvious whether data was 'personal' but in other circumstances it was more ambiguous and open to interpretation. For example, a person's bank details were clearly regarded as personal data. However, 'sanitised' data, which make it more difficult to identify an individual, could still be defined as personal data by the ICO.

For example, the inclusion of credit/debit card numbers within the definition of personal data was raised by a number of participants. One participant was concerned that such card numbers were regarded as personal data even after they had been sanitised (the deletion of most of the digits on paper records of transactions to prevent dishonest copying and use of card numbers). Even if only part of a card number is printed on a receipt it may be possible, with a lot of effort, eventually to match this with another piece of data (such as a name), and this constitutes personal data. One investigator questioned whether it is reasonable to consider information which is so difficult to link to an individual as personal data.

Similarly, participants reported some ambiguity surrounding the interpretation of 'sensitive' data. Many participants stated that different lawyers offer different opinions and that this simply adds to the confusion. The dearth of court cases also means that there can be no certainty about the definition, and reliance has to be placed on lawyers' interpretations and the ICO guidance, which are not always consistent.

Participants from the forensic accounting sector expressed some concerns about data imaging, which is the process of copying computer disks for examination. Such images can contain a whole host of non-relevant personal data or data whose relevance is in doubt. For example, one participant explained that an employee was being investigated in relation to fraud, and the investigator found private correspondence relating to that employee's impending divorce. It could be argued that this data might be relevant, because it could indicate that the employee had financial difficulties that might have been a motive to commit fraud. Others may think this link tenuous. One participant stated that 'we stop looking at non-relevant data as soon as it is realised that it is non-relevant' to avoid contravening DPA 1998. However, the same participant noted of non-relevant personal data stored on a data image that 'you can ignore it but you can't destroy it'.

Data processing

Participants were asked whether there were any problems in relation to data processing and to the respective roles of data controllers and data processors. In most cases participants clearly understood the requirements for legitimate processing and who should be the controller and processor.

For example, when an external party, such as a private investigator or accountant, was involved in an investigation it was usually the data processor, with attendant obligations to stay within the strict bounds of its contract. The company issuing the contract was generally the data controller. Internal investigation departments considered themselves to be data processors and not data controllers, as did credit reference agencies in respect of the data that was passed to them by their clients.[10] This appears to be a misconception. In joint investigations of fraud (e.g. two banks cooperating together) both parties act as data controllers. Participants did not consider that data processing requirements were negatively affecting private fraud investigations.

The forensic accounting firms participating in this research recommended that their clients sought legal advice to clarify each party's roles in this area before commencing any work.

One area of controversy was identified by participants. This was when private investigators act outside of their contract or do not want to reveal their sources. The participants who raised this issue were of the opinion that in these instances the private investigator, and not the client, would be the data controller.

Data retention

Most participants raised concerns over data collected during an investigation that has to be stored for an indeterminate period. Participants from the forensic accounting sector were particularly concerned about data images of employees' computer hard drives, which might contain non-relevant data from an investigation many years ago that could, if released, cause damage to an individual today. One of the forensic accounting participants stated that 'it is technically difficult to erase just parts of a data image, so non-relevant personal data may be around for some time'. Participants stated that there should be some clear guidelines on the length of time data need to be held and also on how data images can be secured to prevent the release of personal and perhaps sensitive data. Forensic accountants were concerned that if this issue was not resolved then they might in future face restrictions to ensure that non-relevant personal data are not gathered during investigation, and that such restrictions might lead to relevant and important data being missed.

Consent

Participants were asked when they would seek explicit consent to gather data, and whether the need for explicit consent had placed any restrictions on the ability to conduct investigations. In summary most participants thought that the issue of consent

[10] The ICO sees credit reference agencies as data controllers; hence subject access requests for credit files are handled by the agencies themselves and not by their clients.

was not a problem. Banks, credit card companies, insurance companies and some employers have clauses in contractual agreements that include explicit consent on the part of an applicant or employee for personal data to be used in a fraud investigation. Many investigations of credit card fraud are designed to protect innocent customers whose identity has been stolen, and in such cases explicit consent is obtained from the injured party, usually without problem.

One forensic accounting firm, when investigating fraud, usually interviewed the suspected employee/director and would get his/her consent at that time. However, the research team believed that the suspect might be more willing to give consent in this situation because it is usually clear that a fraud has been committed, and cooperation may result in internal disciplinary measures rather than a criminal investigation by the police.

Difficulty arises when there is only a suspicion that a fraud may have been committed, and the investigator does not want to alert the suspect by requesting consent. It is in such cases that the exemptions provided by DPA 1998 for obtaining disclosure without consent are useful.

Exemptions

The exemptions available to fraud investigators were discussed in the Introduction, and are fully defined in Annex B. The principal exemption employed by investigators is Section 29, and most participants rarely used other exemptions. However, Section 29 and other exemptions only apply to parts of DPA 1998. This point was raised by both the credit reference agency and the lawyer as very important.

Apprehension over the HRA 1998, a defamation lawsuit, or (in the case of the banks) the *Tournier* case[11] may lead to refusal to disclose regardless of the investigator's claim to exemption. One participant said it 'would not disclose if by so doing they thought they might contravene some other law'.

There appeared to be much confusion in relation to Section 29. A few participants thought that only the police could use it; some thought they could use it only if they had a definite suspicion; and one participant was only vaguely aware of the exemption. This is further evidence to support the view that a general level of confusion, generated through misunderstanding, is making a negative impact on the private-sector investigation of fraud.

One participant made it clear that if an investigator is going to 'trespass into the lives of private individuals' there are degrees of trespass, and all legislation must be engaged; this

[11] *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461. This case also provides guidance for when an information request can be granted.

means more than just DPA 1998. This participant also made it clear that if investigators need to trespass into private lives they should have authority to do that before starting and 'private investigators have to understand this'.

The impact on investigations was clear: Section 29, while providing protection to investigators from parts of the DPA 1998, may still not be enough to guarantee timely disclosure of required data. This led the research team to discuss the sharing of information.

Sharing information

The research suggested that there was a general reluctance to share information, both between private-sector organisations and across private and public sectors.

Participants stated that public bodies such as the Department for Work and Pensions (DWP) and HM Customs and Revenue (HMCR) (except in a few cases) request information regularly, yet are not so accommodating when requests are made to them. In addition, the London Stock Exchange (LSE) closed its information exchange, which included information in relation to habitual bad client risks, as a result of fear of falling foul of DPA 1998.

Criticism was also levelled at private investigators' unwillingness to share data. One participant stated that 'investigators live in a twilight world' and like to protect their sources.

In addition, a major frustration expressed by all non-bank/building society participants was the apparent wish of the banks to make use of data supplied by others while being reluctant to disclose data themselves. One participant described this as a 'facing-one-way attitude'. This raises the wider issue of the banks' social responsibility, which was not within the scope of this research.

Banks have a legal obligation to ensure that the confidentiality of their customers is maintained. However, they are also expected to release data to third parties in appropriate circumstances. Participants from the banking sector said that they would not release data solely on the basis of a Section 29 request.

It appeared that the banks were operating a blanket non-disclosure policy, and this was confirmed by participants from outside the banking sector. A number of reasons for this policy were suggested:

- The banks preferred to disclose only under a court order to avoid any problems that might arise from an incorrect disclosure. It also made it easier to train staff.

- The amount of 'fishing' by private investigators and others using Section 29 was considered unacceptable by banks and building societies. 'Fishing' constitutes requests by investigators for general information not related to a specific case. The level of prevalence of fishing by investigators was unclear.
- There was a general mistrust of private investigators. This led one financial institution to state that it 'would not in any circumstances give data to a private investigator'.
- Banks have for many years protected client confidentiality and use the *Tournier* case as a defence, so that even if a Section 29 request may be on the face of it acceptable, client confidentiality will always prevail.
- Banks were reluctant to share any information in cases where they had not suffered a loss themselves. The view of the banks was that the investigator would have to prove that their client had committed a fraud before they would release data.
- Sharing of information between banks and building societies was done on an informal, non-traceable basis, facilitated by relationships between fraud investigation teams. One participant made it clear that sharing data 'really depends on who approaches you'. Another participant stated that they 'might put the word out' if there was an active fraudster doing the rounds.
- The credibility of the investigator was important. The participants stated that the police have more credibility because they have extensive training and are regulated. Banks and building societies were asked whether they would be more willing to share information if private investigators were properly licensed and trained, and the response was generally positive, provided the banks had confidence in the regulatory regime (training, licensing, censorship and penalties similar to those under which the police operate).
- Banks (and indeed many clients) generally did not want it known that they suffered from fraud, and it was normal practice to account for such frauds as market risks or bad debts in order to mitigate the risk of reputational damage. It has been estimated that reputation can be worth up to 70 per cent of a company's market value.[12]

These factors may increase the length of time required to conduct private-sector fraud investigations. Therefore the researchers believe that a more open and cooperative approach to sharing information is required.

Credit reference agencies

All participants had dealings with credit reference agencies, and in the main had a good relationship with them, particularly with those that are also members of CIFAS – the UK's Fraud Prevention Service (CIFAS).[13]

[12] Larkin, J. (2003) *Strategic Reputation Risk Management* Basingstoke: Palgrave Macmillan.
[13] At *http://www.cifas.org.uk/*

There seemed to be some misunderstanding on the part of some participants about 'footprints' (records of searches) left on accounts when a Section 29 request is made. For example, one participant spoke of an investigation that had been compromised because a footprint was left on an account, and the account holder made a subject access request which suggested that an investigation was in process. The credit reference company claimed that it was up to the investigator to have this request removed to prevent it being visible to the subject. Some participants were not aware of the ability to remove Section 29 footprints.

Another point misunderstood by some participants is that Section 29 does not guarantee that information will be given (see above), and the credit reference agency felt obliged to mirror the practice and law followed by its clients.

Police involvement

The police were perceived by most participants as being afforded greater powers and respect than private investigators. They would not normally, for example, have any difficulty in defining their role as being concerned with the prevention and investigation of crime, which is not always the case for private-sector investigators, especially during the early stages of an investigation.

The police can also cut through some barriers more quickly and obtain court orders more easily. The willingness of the police to get involved can thus affect the degree to which DPA 1998 affects fraud investigations.

Yet the police were seen as reluctant to become involved in private-sector fraud investigations, and as potentially neutral on fraud resolution. In most cases participants stated that the police would be interested in a fraud case only if 95 per cent of the investigatory work had been done by an internal or private investigator and/or when there was good chance of a quick clear-up.

Participants cited a number of reasons why, in their view, the police were reluctant to take on fraud cases:

- Fraud detection does not count in police 'key performance indicators' (KPIs), nor is fraud counted in the British Crime Survey, which has become an important barometer in measuring crime in the UK.
- The police do not like to be seen as debt collectors.
- The jurisdiction in which a fraud occurs can be in doubt. For example, a fraud committed against a person who lives in London by a person in Birmingham on a credit card company based in Northampton can create a dispute over where the

offence took place, and thus which police force should take the case. Participants indicated that 'playing ping-pong' with various police forces was very frustrating.

- Because frauds can be resource-hungry, larger frauds were more likely to be taken on by the police than smaller frauds. The participants suggested that the cost/benefit, and associated kudos, is much higher with higher-profile fraud cases.
- There was no police national fraud team, and local resources are fully deployed on crimes that count towards KPIs.

It is important to note that the views of the police were not sought as part of this research project. Consequently the views above are only those of participants. A few participants indicated that they had a good relationship with the police and that their cases had generally been accepted.

The role of the Information Commissioner's Office (ICO)

All participants considered that the ICO played a pivotal role in giving guidance on DPA 1998, and could have a significant effect on how a fraud investigation is conducted. All the definitions in Annex B come from the legal guidance provided by this Office. Feedback from participants on the value of this guidance was mixed.

Positive comments made by participants in relation to the ICO included:

- Some participants were entirely content with the Office.
- Staff of the Office were prepared to come out and meet organisations to discuss issues.

However, criticism also emerged from the interviews in the following terms:

- Advice was often too general and vague, leaving doubts in the minds of practitioners.
- There was a tendency to quote the law back at enquirers, which was not considered helpful. Participants suggested that what is needed is practical advice that can be used in the field.
- Advice differed and was inconsistent, depending on whom practitioners spoke to, and at what day and time they spoke. Some participants made it clear that they would keep telephoning until they got the answer that they wanted, and follow this up with a confirmatory letter or email. It seemed to the researchers that only the very persistent will make any headway, and then may act on incorrect advice.
- More consideration needed to be given to investigators and the need to investigate fraud, and for this to be balanced with the requirement to protect personal data. Participants claimed that the private sector dedicates a huge amount of resources to fraud investigation and prevention, often exceeding many police forces' budgets.

Consequently, the ICO ought to accord the work of investigators greater respect in protecting the public good.

- Most participants felt that the Office should issue a statement that organisations have a right to protect themselves against fraud. It was believed that this would add weight to requests for information to combat fraud and would reinforce exemptions.
- Participants clearly thought that better guidelines were required, especially in relation to crime prevention systems. In general the ICO asserts that each data request should be considered on a case-by-case basis, but crime prevention systems review data on an ongoing basis. For example, a system that is monitoring sales transactions at a point-of-sale in a store contains personal data (the cashier's ID) to detect fraud. The system will continually examine all data even though the vast majority of staff are not committing any fraud. Although there were some guidelines concerning crime prevention systems, for example on CCTV, more were required. The researchers thought that if guidelines were produced this might also alleviate the problem of inconsistent advice. Participants wanted more concrete assurance that their crime prevention systems were not contravening DPA 1998.
- Overall, it appeared that the actions or (sometimes) inaction of the ICO added to the level of misunderstanding and apprehension mentioned earlier, which feeds a reluctance to share data and impedes private fraud investigation. This is because the lack of clear definitions and guidance creates fear of the consequences of getting it wrong.

The ICO was not consulted as a part of this research. At present, the views are only those of the participants. However it should be noted that as a result of the *Making Data Protection Simpler* project[14] the Office is planning to establish a Guidance and Promotion Division to develop a more proactive approach to providing more relevant and practical advice. In addition the Office conducts annual surveys with both businesses and individuals to assess the level of knowledge and understanding of data protection.[15]

Other legislation

The level of knowledge of other legislation, such as the HRA 1998, FOI 2000, Regulation of Investigatory Powers Act 2000 (RIPA 2000) and other statutes, varied between participants. However, most participants did not have knowledge of recent cases in the human rights arena (e.g. *Jones v the University of Warwick*[16] or *Douglas v Hello Ltd*[17]) or of those that might impact on fraud investigations.

[14] Information Commissioner's Office (2005) *Making Data Protection Simpler*, 13 March 2005.
[15] Information Commissioner's Office *Annual Track and Customer Satisfaction Surveys*. At *http://www.informationcommissioner.gov.uk*.
[16] [2003] EWCA (Civ) 151.
[17] [2003] EWHC 786 (Ch); [2005] EWCA (Civ) 595.

One participant thought that RIPA 2000 was very badly drafted, claiming that as a result Royal Mail (in relation to mail redirection) had misinterpreted Part I Chapter II of this Act, leading to difficulty in tracing fraudsters to their new addresses.

According to participants the plethora of new legislation is causing great confusion. For example, the laws against money-laundering cut right across the DPA 1998, since 'disclosure [of a 'suspicious activity report' (SAR) to a data subject suspected of being involved in money-laundering] would be likely to prejudice any investigation which might be conducted following the making of the SAR'. Guidance issued by the Treasury suggests that subject data requests in cases of suspected money-laundering may be covered by Section 29,[18] and if so should not be disclosed during a subject access request. Many participants perceived that there was an emphasis in legislation on crime prevention measures to counter money-laundering which was not evident for private fraud investigations.

Many participants were concerned about the impact of the FOI 2000 on investigations. However, in the view of the research team this seems to stem from a lack of familiarity with the legislation, especially with Section 30, which specifically exempts information held for investigative purposes. The applicability of FOI 2000 to the private sector was also unclear. This is just another factor that might contribute to a general level of misunderstanding and apprehension of the DPA 1998. Recent discussion in relation to the FOI 2000 suggests that many organisations are not prepared for its impact.[19]

Participants were also concerned by the conflict between EU directives and the DPA 1998: for example, the conflict with the Directive on Consumer Credit. This means that compliance with one piece of legislation may conflict with compliance with another.

Eighth Principle of the DPA 1998: data sent outside the European Economic Area (EEA)

Most participants did not typically send data outside the EEA, and therefore did not have a significant issue with the eighth principle, which prohibits the transfer of personal information to countries outside the EEA. However, there was some concern about global companies and the exchange of information which has yet to manifest itself in practice. Two issues raised by some participants were that:

- Some EU countries may be reluctant to send information to the UK if they perceive that the DPA 1998 is not 'good enough' to protect them against claims that they were acting out of step with their own requirements.
- There did not appear to be a list of countries to which data should not be exported.

[18] At *http://www.hm-treasury.gov.uk./media/112/23/money_laundering.pdf.*
[19] At *http://www.FT.com/HomeUK* – 'Companies not ready for public information law change', 18 November 2004.

Although no such list exists, the Europa website contains an up-to-date list of countries and territories that the European Commission has deemed to have an 'adequate' level of protection. Transfers to these countries and territories, and to companies in the USA that have signed up to the 'Safe Harbour' arrangement, do not breach the eighth principle.[20]

General comments of participants

Participants also identified a number of other issues that were seen to impact on the investigation of private-sector fraud:

- Investigations now take much longer to conduct under the DPA 1998. One participant said, 'You have to go through more hoops now'. More work means more cost, and the law favours the fraudster rather than the victim.
- The new SIA[21] licensing arrangements do not apply to internal investigators. This is seen to put private investigators at a disadvantage.
- Fraud is seen as a victimless crime, when in fact many people have to pay for it.
- For the forensic accounting firms the main aims of investigations are to recover money and prevent future similar losses. This means that some major frauds go unreported and unprosecuted.
- One participant thought that it was 'not such a bad piece of legislation'.
- Human resource departments are quite often reluctant to release data, even when a Section 29 request is made.

General observations

During the research a number of general observations were made by the research team on the factors that determine whether or not an organisation is likely to be successful in obtaining disclosure. These factors need further examination, but are nevertheless worthy of mention:

- Those organisations that appear to have good procedures and policies in place tend to have fewer problems with fraud investigation or obtaining information. These organisations have forms and procedures for a wide range of eventualities.
- The better an investigation team is at building internal and external relationships, the better results it achieves in acquiring data.
- Trust plays an important role in the release of data. Trust gives organisations confidence to release data to other parties.

[20] At *http://www.europa.eu.int/*
[21] At *http://www.the-sia.org.uk/*

Participants' views on what is needed

Participants were asked what was needed to improve the current situation and make investigations easier to conduct, without affecting the rights of individuals. These are the views of the participants; they have not been subject to any detailed critical analysis:

- The ICO needs to provide more practical guidelines, with scenarios of good and bad practice, to inform the investigative process.
- Greater professionalism is required of investigators, along with appropriate training and examination.
- Easier availability of certain data, in particular that relating to deceased persons and to passports and driving licences.
- The SIA needs to apply stringent licensing requirements to investigators, both private and in-house.
- An effective lobbying group is required to represent all investigators, to get the appropriate changes in legislation.

Conclusions

This research suggested that, following the enactment of DPA 1998, investigations can take longer and be more costly and more difficult to accomplish successfully than before. However, our research was unable to establish conclusively whether this was a direct result of a correct application of the legislative provisions of the Act and/or its interpretation by the courts, and/or the result of the way it is being interpreted by data handlers. We were able to observe that some data handlers appeared to rely on DPA 1998 to justify refusal to disclose data despite the provisions of Section 29 which allow disclosure for the purpose of assisting in the detection and prosecution of criminal offences.

In summary the main conclusions of the research are:

- Participants considered a lack of proper understanding of the provisions of DPA 1998 is leading to a presumption in favour of non-disclosure of data and a consequent compromising effect on private-sector investigations of allegations of fraud, particularly in relation to information about deceased persons.
- There was a perception of a lack of clarity in the provisions of DPA 1998 itself. A lack of judicial authority in this area further exacerbates the problem. Data controllers are perceived to be 'hiding behind the Act' to justify their non-cooperation in private-sector fraud investigations.
- Provisions relating to definitions (including what data were covered by the Act), data retention and exemptions (particularly section 29) were perceived as the most problematic by participants. Data-processing and consent requirements were not considered to restrict private fraud investigations.
- Participants suggested that more guidance on the application of DPA 1998 would be helpful. The ICO were considered to play a pivotal role in the provision of such advice.
- Those organisations that appear to have good procedures and policies in place tend to have fewer problems with fraud investigation or with obtaining information. These organisations have forms and procedures for a wide range of eventualities.
- There was a general consensus that there needs to be more effective regulatory control over both internal and external investigators, who are currently not subject to any effective form of control.
- The better a team is at building internal and external relationships, the better results it achieves in acquiring data.

- Trust plays an important role in the release of data. Trust gives organisations confidence to release data to other parties.
- Fraud was not considered to be a priority for law enforcement. The police were perceived to be reluctant to investigate allegations of fraud in the private sector unless most of the investigatory work had already been completed.
- There was a general reluctance to share information with other organisations. Banks were particularly wary of releasing information to private investigators.

Annex A: Fraud Advisory Panel interview schedule

1. Are you aware of the definition of data in the Information Commissioner's legal guidance on the DPA?

2. Are you familiar with the principles of the *Durant* case? (If not, explain briefly.)

3. Is it clear, in your opinion, what data is covered (manual, automated, internet, provided by third parties, CCTV, etc)?

4. What, if any, are the causes for concern?

5. In most cases are the roles and responsibilities of the data controller and data processor clear?

6. In the case of an investigation where more than one party is involved who, in your experience, assumes the role of the controller? What complications arise, if any, in deciding who the data controller is?

7. During an investigation, where a company commissions an investigation who is normally the data controller, and why?

8. At what stage of an investigation (if at all) would explicit consent be required from a person who is the subject of an investigation?

9. In your view, what restrictions do the need to request 'explicit' consent place on the ability to conduct a successful investigation?

10. Are you aware of the exemptions offered by Section 29 of the Act? (If not, briefly outline.)

11. How do you think (if at all) the Section 29 exemptions offer protection to the investigation process?

12. There are a number of phases to an investigation which may or may not start with an event which arouses some kind of suspicion. In your experience, what are the main stages of an investigation, and how would you approach the collection of information?

13. If an investigation might indicate potential criminal activity, at what stage would you involve the police, and why?

14. In your experience, what are the types of response you receive from the police (when you request their involvement), and why do you receive these responses?

15. During an investigation what sort of requirements are placed on you as an investigator by the police (if any)?

16. What impact, if any, does other legislation have on your investigations (e.g. the Freedom of Information Act, RIPA and HRA), given recent legal decisions such as *Zeta Jones and Douglas v. Hello Magazine*? (If not familiar these will be outlined briefly to the interviewee.)

17. What other problems do you face in relation to the DPA and investigations?

Annex B: Definitions

These definitions are taken directly from the legal guidance notes published by the Information Commissioner's Office. (The numbering appearing in some of the headings below reflects the numbering in the ICO legal guidance notes.)

Personal data

Personal data are defined in the Act, at section 1(1), as follows: 'data which relate to a living individual who can be identified:

- from those data; or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.

Data controller

'[A] person who (either alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed'.

Data processor

'Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.'

Section 29 exemptions

5.3.1 The first crime and taxation exemption (section 29(1))
Personal data processed for any of the crime and taxation purposes are exempt from –

- the First Data Protection Principle except that part which requires compliance with the conditions for processing and the conditions for processing sensitive data; and
- subject access

to the extent to which the application of those provisions to the data would be likely to prejudice any of the crime and taxation purposes. In other words, the data controller must not disregard those provisions unless their application would be likely to prejudice any of the crime and taxation purposes.

5.3.2 The second crime and taxation exemption (section 29(2))
Personal data which –

- are processed for the purpose of discharging statutory functions; and
- consist of information obtained for such a purpose from a person who had it in his possession for any of the crime and taxation purposes

are exempt from the subject information provisions to the extent to which the application of the subject information provisions to the data would be likely to prejudice any of the crime and taxation purposes.

5.3.3 The third crime and taxation exemption (section 29(3))
Personal data are exempt from the non-disclosure provisions in any case where the disclosure is for any of the crime and taxation purposes and where the application of those provisions in relation to the disclosure would be likely to prejudice any of the crime and taxation purposes.

5.9 Disclosures required by law (section 35(1))

Where the disclosure is required by or under any enactment, by any rule of law or by the order of a court, personal data are exempt from the non-disclosure provisions.

In these circumstances, the legal obligation overrides any objection which the data subject may have, but an element of fairness can still be applied.

For example, if the data controller is well aware when he collects the data that at some point he is likely to have to make disclosures of those data under statute, it would not be incompatible with the disclosure to notify data subjects at the time the data are collected from them, that such disclosure is likely. The First Principle should not be disapplied generally.

5.10 Disclosures made in connection with legal proceedings (section 35(2))

Where the disclosure is necessary –

- for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings); or
- for the purpose of obtaining legal advice; or
- is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

personal data are exempt from the non-disclosure provisions.

A data controller is not obliged to disclose personal data pursuant to a request made by a third party under section 35(2).

This provision affords the data controller exemption from any or all of the non-disclosure provisions in cases where:

- the data controller is satisfied that the nature of the request is such that the disclosure of the personal data falls within this section i.e. the disclosure is necessary for one or more of the above, and
- the data controller is satisfied that to apply the particular provision would be inconsistent with the disclosure in question.

The data controller has to remember that Schedule 2 and (where the processing is of sensitive personal data) Schedule 3 still have to be complied with. In many cases, the data controller will not be in a position to make a decision as to whether the necessity test can be met, or will not wish to make the disclosure because of his relationship with the data subject, with the result that the requesting party will have to rely upon a Court order to obtain the information.

Schedule 7: some exemptions

5.17 Management Forecasts/Management Planning

This exemption is available to businesses to protect confidentiality of personal data processed for the purposes of management forecasting or management planning. In any case to the extent to which the application of any of the subject information provisions to personal data processed for such purposes would be likely to prejudice the conduct of the business or other activity of the data controller, such personal data are exempt from the subject information provisions.

5.22 Legal professional privilege

If personal data consist of information in respect of which a claim to legal professional privilege (in Scotland, confidentiality as between client and professional legal adviser) could be maintained in legal proceedings, the personal data are exempt from the subject information provisions forever unless the privilege is waived.

Information a lawyer receives in the course of advising his client is confidential and should usually only be disclosed with the client's authority.

Annex C: Biographies

Professor Martin Gill: Director PRCI

Martin Gill is Director of Perpetuity Research and Consultancy International and a Professor of Criminology at the University of Leicester. He has published over 100 journal and magazine articles and 11 books, including *Commercial Robbery*; *CCTV*; and *Managing Security*. He is co-editor of the *Security Journal* and founding editor of *Risk Management: an International Journal*. Professor Gill is a Fellow of The Security Institute and a member of the Risk and Security Management Forum, the Company of Security Professionals (and therefore a Freeman of the City of London), Chair of the ASIS Research Committee, and an overseas representative on the ASIS International Academic Programs Committee. He is also a member of the Fraud Advisory Panel and Association of Certified Fraud Examiners. He has just produced two reports; one based on interviews with fraudsters in prison and the other on the impact of US legislation on ID fraud (both published on the PRCI website). He has also assessed victims' perspectives on ID fraud. Martin is also working with the security industry to assess the value of security.

Doug Smith: Head of Security and Risk

Doug is a specialist in risk and security services, including the use of technology. He has extensive international experience (e.g. United States, United Kingdom, Brazil, Argentina, Mexico, France and Spain). He holds an MSc in Risk Crisis and Disaster Management from Leicester University and an Executive MBA from Oxford Brookes University.

Martin Hemming: Research Associate

Martin has an MSc in Security Management and a bachelor's degree in law from King's College London. He has 12 years' experience with the Post Office Investigation Department, and has contributed to a range of PRCI projects.

Perpetuity Research & Consultancy International (PRCI) Ltd
148 Upper New Walk, Leicester LE1 7QA, UK

Tel: +44 (0)116 222 5555 Fax: +44 (0)116 222 5557
Email: prci@perpetuitygroup.com www.perpetuitygroup.com

For more information on the Fraud Advisory Panel please contact:

Fraud Advisory Panel
Chartered Accountants' Hall, PO Box 433, Moorgate Place, London EC2P 2BJ

Tel: 020 7920 8721
Fax: 020 7920 8545
Email: info@fraudadvisorypanel.org

Or visit:
www.fraudadvisorypanel.org

Registered Charity No. 1108863

March 2006

OTHPLN5152 3/06