Stolen identity: regulating the illegal trade in personal data in the 'data-based society'

Dr Adam Warren (PhD, MA, BA)

Department of Information Science
Loughborough University
Loughborough
Leicestershire
LE11 3HZ
United Kingdom

Tel: +44 (0)1509 223074
Fax: +44 (0)1509 223053
Email: a.p.warren@lboro.ac.uk

Abstract

In May 2006, the UK Information Commissioner's Office (ICO) presented a report to Parliament entitled *What Price Privacy?* The report highlighted the extent of the illegal trade in personal data. Arguing that the risk of security breaches had increased largely as a result of the rise of the 'data-based society', the ICO called for a change in the legislation to permit jail sentences of up to two years in respect of offences under section 55 of the Data Protection Act 1998. In February 2007, the UK government stated its intention to adopt that recommendation.

This paper examines the current UK policy approach to regulating the illegal flow of personal information, and the lead taken by the UK Information Commissioner. Reference is made to the 'privacy toolbox', where data protection legislation is combined with measures such as codes of practice and privacy impact assessments (PIAs). Comparisons are made with the work of overseas regulators. In addition, the current regulatory framework regarding section 55 offences is examined, with the author attending an ICO prosecution hearing in December 2006. The paper concludes by arguing that a greater emphasis needs to be placed on the assessment of privacy risks posed, in particular, by the expansion and proposed merger of government databases. Adoption of PIAs could help achieve this.

This article was submitted on 14 February 2007, and updated on 4 May 2007.

Stolen identity: regulating the illegal trade in personal data in the 'data-based society'

1. Introduction

In May 2006, the UK Information Commissioner's Office (ICO) used its powers under section 52(2) of the Data Protection Act (DPA) for the first time to present a report to Parliament. The publication, *What Price Privacy?*, highlighted the extent of the illegal trade in personal information as diverse as current addresses, ex-directory telephone numbers or records of calls made, criminal records and bank details.[1] The report added that the growth of the 'data-based society' increased the risk of further security breaches. Although section 55 of the DPA 1998 made it an offence to 'knowingly or recklessly' obtain, disclose or 'procure the disclosure' of personal information without the consent of the organisation holding the data, the ICO argued that the existing non-custodial penalties offered little deterrent.[2] The report therefore called for a change in the legislation to permit jail sentences of up to two years for those convicted of section 55 breaches. In February 2007, the Department of Constitutional Affairs (DCA) stated its intention to adopt the ICO's recommendations.[3]

This paper examines the current UK policy approach to regulating the illegal flow of personal information, and the lead taken by the UK Information Commissioner. Reference is made to the 'privacy toolbox', where government data protection legislation has been combined with data protection supervisory authorities, codes of practice, privacy impact assessments (PIAs) and technological solutions.[4] It is argued that, with the UK government supporting its proposals to amend the DPA 1998 to combat illegal data sharing, the UK ICO is taking a greater role in the formation of policy in this area, although in other areas of policy they lag behind privacy regulators in countries such as the Netherlands, Canada and New Zealand. This article begins by outlining some recent developments that have transformed the UK into a 'data-based society'.[5] Attention is paid to the promotion of greater joined-up working between government agencies, and the gathering of data originally collected for distinct purposes in new databases such as the Children's Information Sharing Index. The creation of single, comprehensive repositories not only enhances the ability of the government to monitor its citizens, but also presents great opportunities for illegal data sharing. Although the UK government have decided against constructing a single National Identity Register system,[6] the launch of a significant policy review in January 2007 into sharing information across government departments has led to accusations that a single 'super-database' will indeed be created.[7] Additionally, consideration is given to the security of personal information held in the private sector, where databases have been built up by retailers, telecommunications companies, utilities and financial institutions.

Secondly, the current regulatory framework regarding section 55 offences is examined. Attention is given to the enquiries conducted by the Commissioner as part of Operation Motorman, which underpinned the recommendations set

out in *What Price Privacy?*, and the follow up report published in December 2006.[8] The author gained further insight into the existing prosecution process through attendance of an ICO prosecution hearing in December 2006.[9] In addition to the report's main recommendation on custodial sentencing, attention is given to other suggested measures - such as inter-agency protocols and addendums to professional codes of ethics - that the ICO are also trying to promote as part a balanced 'privacy toolbox'. The role of Privacy Impact Assessments (PIAs), well established in jurisdictions such as Canada and New Zealand and long advocated by the ICO, are given serious consideration.

This paper concludes by assessing the changing role of the UK data protection supervisory authority. Comparisons are drawn with overseas data protection regulators, where the emphasis is on anticipating privacy risks posed by information systems.

2. The 'privacy toolbox'

In their analysis of data protection legislation, Bennett and Raab (2006) discussed regulatory interdependence, in which a nation's public policies to protect personal privacy are linked with the actions of public and private organisations that operate outside its borders.[10] However, whilst laws have increasingly converged around a substantive set of international standards – the most important being the 1995 European Union (EU) Data Protection Directive – the way they have been implemented in practice has resulted in divergences, as well as doubts as to the effectiveness of statutory approaches in coping with rapid technological developments that have significant consequences for privacy.[11] It has been suggested that tools such as codes of practice, PIAs and privacy enhancing technologies (PETs) provide a flexible means of improving data protection compliance.

Discussion of these tools is limited by space, but it is worth stating that they have been developed to good effect overseas. The Netherlands, for example, has a tradition of using codes of practice[12] and PIAs have been developed in the private sector by Royal Philips Electronics to ensure compliance of global IT systems.[13] Moreover, the Netherlands has collaborated since the mid-1990s with the Canadian province of Ontario over the appraisal of technologies for protecting privacy.[14] However, progress has been slow in the UK. The UK data protection regulator was not granted authority to develop codes of practice until the DPA 1998 came into effect in 2000.[15] Moreover, ICO and expert calls for the development of PIAs, particularly in relation to the National Identity Register, have so far gone unheeded.[16] However, as governments and businesses came to terms with the introduction of new information systems and the convergence of existing technologies there is strong case to be made for a combination of privacy measures covering collection, storage, security, sharing and management of personal information.

3. Databases and data security

Under the slogan 'joined-up government', the UK government has over the period of a decade stated its commitment to greater coordination and integration of public services. This began with the *Modernising Government* white paper,[17] and was developed further in the policy papers: *Privacy and data sharing* (Cabinet Office, 2002),[18] and *Transformational Government*.[19] The latter called for three key 'transformations' towards:

- *Citizen and business centred services*, improving choice of interaction with public services;
- *Shared services* across the public sector, including human resources, finance, information management and customer service. This would improve efficiency and reduce duplication, for example, by slimming down the 130 central government call centres;
- *Professionalism* including the appointment of Customer Service Directors and improving the management of information technology programmes.

The paper outlined a broad programme, continuing beyond 2011, towards a vision where 'boundaries between departments, between central and local government, and between public, private and voluntary sectors become less important and less visible to the citizens and business' (Cabinet Office, 2005: 18-19).[20]

A number of agencies and teams have been established to deliver on government aspirations. For example, the Department for Health established NHS Connecting for Health in April 2005 to deliver the National Programme for IT, aimed at integrating systems connecting over 100 000 doctors, 380 000 nurses and 50 000 other health professionals in order to provide patient-centred care.[21] Progress to date has been mixed.[22] Within the Department for Education and Skills, a project team has been established to set up the Children's Information Sharing Index - a database of England's 11 million children, accessible to 'authorised practitioners' in education, health, social care, youth offending and some voluntary services.[23] Information held will include the child's name, address, date of birth, an identifying number, and details of schools, GPs and parents or carers. It is due to be operational by the end of 2008.

However, concerns have been raised that the promotion of shared services, particularly where children's data is involved, can cause 'actual harm'.[24] Three decades ago, Rule had written about the attractiveness to governments, and perhaps inevitability, of systematic cooperation between individual surveillance systems:

> The effect of such cooperation, when it does occur, is distinctly to enhance the position of the systems of control vis-à-vis their clienteles, to increase their surveillance capacity, and to conduce to change in the relations between agencies of surveillance generally and the public at large.[25]

The establishment of a National Identity Register (NIR) under the Identity Cards Act 2006 arguably turns what Rule termed a 'symbiosis' of surveillance systems into a reality. Information will be held on three existing IT systems[26] and may include personal information, residential information, identification information (such as signature and biometric data), personal reference numbers (for example, national insurance and passport numbers), record history and details of when a Register entry has been accessed and people to whom such information has been provided. Although this represents a change from the previous policy of holding data on a single information system, some campaign groups expressed concerns that security would be further compromised as the new NIR will involve 'mixing up' new data with existing data.[27]

In the private sector, the security of confidential information held by utilities, telecommunications companies and financial service providers among others has come under scrutiny. Supermarkets have long held databases of customer shopping habits, and Tesco's suffered adverse publicity after piloting tiny location-identifying RFID tags.[28] Yet, in spite of this, investment in security standards and related qualifications remains low. According to a study commissioned by the Department of Trade and Industry (DTI), three fifths of UK businesses are still without a security policy, and just 44% of companies had conducted security risk assessments in the previous year.[29] More worrying, at a time when more customers and suppliers are granted direct access to corporate systems, 30% of transactional websites do not encrypt the transactions that pass over the internet.[30]

Clearly, opportunities exist for organised and opportunist criminals. Much of the personal information held in both public and private sectors is accessible either online or via call centres. And, as the recent cloning of a biometric passport demonstrated, even the heavily promoted RFID technology available is far from secure.[31]

4. *What Price Privacy?*

Context

The above developments are important, describing the societal context in which the ICO currently operates. Nevertheless, according to ICO solicitor Philip Taylor, it was frustration experienced by an ICO prosecution under section 55 of the DPA 1998 in the summer of 2005 that caused the Commissioner to present a special report to Parliament.[32]

Legal proceedings had started after the ICO attended a search of premises in Surrey in late 2002, under a warrant issued by Devon and Cornwall Constabulary. The raid concerned the suspected misuse of the Police National Computer (PNC) by serving and former police officers.[33] However, vehicle registration numbers found at the scene suggested that the suspect also had an 'inside track' to the Driving and Vehicle Licensing Agency (DVLA).

This resulted in the ICO launching an investigation dubbed 'Operation Motorman' into data protection offences,[34] and to a raid of the premises of a private detective working in Hampshire. Documents seized revealed a network of contacts illegally acquiring information on the private detective's behalf based at British Telecom, the DVLA and the PNC. Other papers included correspondence between the detective and journalists working for a number of prominent national newspapers and magazines. The information supplied by the private detective to his clients included details of criminal records, driving licence data, ex-directory telephone numbers and mobile phone records. This evidence, together with the suspect's detailed records of work carried out, 'documented literally thousands of section 55 offences'.[35]

In all, the ICO activity under Operation Motorman resulted in the Crown Prosecution Service (CPS) charging four people with corruption offences, including the private detective. Two pleaded guilty to corruption charges and two to charges under section 55 of the DPA 1998. However, the issuing of a suspended sentence to the first defendant in this case, a police civilian worker, 'frustrated' the subsequent ICO prosecution by setting a precedent for the 'lesser' section 55 offences, for which the court was unable to impose any sentence stronger than a conditional discharge.[36] As the ICO stated in *What Price Privacy?*:

> This was a great disappointment to the ICO, especially as it seemed to underplay the seriousness of section 55 offences. It also meant that it was not in the public interest to proceed with the ICO's own prosecutions[37], nor could the Information Commissioner contemplate bringing prosecutions against the journalists or others to whom confidential information had been supplied.[38]

Recommendations

The ICO reported on the issue in May 2006, with *What Price Privacy?* receiving wide media coverage[39]. The report's central recommendation was for the introduction of custodial sentences of up to two years for persons convicted on indictment and up to six months for summary convictions. The aim was to 'discourage this undercover market and to send out a clear signal that obtaining personal information unlawfully is a serious crime' (ICO, 2006a: 5).[40] The ICO stated that the police supported the threat of imprisonment as a suitable deterrent. Under the existing system, the police have to arrest for malfeasance or corruption offences in order to secure a custodial sentence. In future, they would prefer to use section 55 as the basis for their investigations and believe that they would achieve quicker convictions, if custodial sentences were introduced.

Further recommendations stated that:

- The Security Industry Authority[41] should include a caution or conviction for a section 55 offence among the grounds for refusing or revoking the licence of a private investigator;
- The Association of British Investigators[42] should extend its National Occupational Standard for Investigation to include explicit reference to

section 55 offences, and undertake other specific measures aimed at raising standards among private investigators;
- The Press Complaints Commission (PCC) should take a much stronger line in tackling press involvement in the illegal trade;
- The ICO will not hesitate to prosecute journalists identified in previous investigations who continued to commit section 55 offences;
- The Office of Fair Trading should amend its 2003 Debt Collection Guidance - directly linked to fitness to hold a consumer credit licence - to condemn section 55 offences.[43]

The press came in for particular criticism in *What Price Privacy?* with the report referencing the House of Commons Select Committee on Culture, Media and Sport's investigation into privacy and media intrusion. The Select Committee had not been convinced by the press's compliance with codes of conduct, concluding with a list of intrusive data-gathering practices that amounted to 'a depressing catalogue of deplorable practices'.[44] The ICO also cited examples retrieved during their Operation Motorman investigation, where records contained personal data of individuals who had either tenuous links with the celebrity circuit or had no obvious newsworthiness. The Commissioner reported this emerging evidence to the PCC, who 'issued a Note reminding the press of its data protection obligations, including the possibility of committing an offence when obtaining personal information'.[45]

Finally, the report concluded by inviting a number of regulatory and professional bodies that appeared 'to exercise control or influence over those who may engage in the buying or selling of personal information' to respond to specific questions about the steps they will take to achieve good practice in their information trading activities.[46] The ICO also requested responses and further evidence from consumer and citizens' organisations.

Reaction and government consultation

According to Taylor, the reaction from the media was 'more positive than expected' given the criticism the report levelled at the profession.[47] However, despite the PCC issuing a further reminder in August 2006 to journalists about their obligations under its code of conduct, the press self-regulator has been criticised for its unwillingness 'to instigate an inquiry of its own' into illegal trawls for personal data.[48] In fact, the imprisonment of Clive Goodman in January 2007, royal editor of the *News of World*, for conspiring to intercept voicemail messages in the Prince of Wales' household demonstrates that journalists have continued to flout the law in this area.[49] Generally, the 'broadsheet' press were supportive of the ICO report and recommendations with *The Observer's* coverage being singled out as being especially positive. The more 'popular' press, whilst agreeing that the illegal practices were undesirable, were reluctant to support the imposition of custodial sentences.[50]

In July 2006, the DCA published a consultation paper proposing to amend the DPA 1998 to allow custodial sentences matching the recommendations of the ICO report.[51] The consultation paper sought views on whether the amendments:

- Represented a proportionate sanction for the courts to be able to use;
- Acted as an effective deterrent to those who unlawfully trade in and otherwise deliberately or recklessly misuse personal information.[52]

The consultation period ended in October 2006. In proposing the amendments, the government sought to reinforce their data sharing agenda by demonstrating the security of personal information once it had been shared. Thus, increasing the penalties available to the courts would:

- Provide a greater deterrent to those who seek to knowingly or recklessly disclose or procure the disclosure of confidential personal information without the consent of the data controller;
- Provide public reassurance that those who are successfully prosecuted may, dependent on the gravity of the offence, be sent to jail;
- Achieve parity of approach across a number of disparate pieces of legislation which deal with similar type offences.[53]

Essentially, the government viewed the introduction of custodial sentences for a section 55 offence as a harmonising measure, whereby the Data Protection Act 1998 'sets the standards for offences relating to the wilful misuse of personal information' across the public and private sectors.[54] Examples where custodial sentences had already been put in place for specific offences relating to misuse of personal data included:

- The Identity Cards Act 2006 (section 27) for unauthorised disclosure of information from the NIR, once implemented;
- The Social Security Administration Act 1992 (section 123) for misuse of personal data;
- The Commissioners for the Revenue and Customs Act 2005 (section 18(1) and 19(1)) for unauthorised disclosure by Revenue and Customs officials.

Safeguards would be built in to protect people who were deceived into disclosing information they believed they had the legal right to release.

In its assessment of the potential impact of the proposed changes, the DCA noted that section 55 cases did not often end up in court, that just 26 prosecutions had had been taken forward in the last four years. Of those, only five were serious enough to warrant prosecution in the Crown Court. The government did not consider that the creation of the new sanction would cause the level of prosecutions to rise 'as the offence is already in existence and has a prosecution history'. Consequently, in February 2007, the DCA confirmed that section 60 of the DPA 1998 would be amended to permit custodial sentences for section 55 offences 'as soon as parliamentary time allow[ed]'.[55]

5. Current prosecution process and follow-up report

The Clifford case

The Clifford case, involving the prosecution of a private detective in Surrey, is typical of those highlighted by the ICO and DCA. Anthony Clifford of Chessington, Surrey obtained and sold information on a number of individuals through his private investigation agency trading as MRS. He impersonated officials to 'blag' personal information from companies and banks. A search of his premises resulted in the seizure of some 250 investigation files consisting mainly of requests for bank account details, mortgage account details, credit card statements, itemised telephone billing and credit reference checks.[56] Additionally, Clifford used a female employee to obtain personal information relating to a number of women.

In all, Clifford pleaded guilty to 16 counts of illegally obtaining and selling personal information under section 55 of the DPA 1998 and to a further offence of failing to notify his data processing activities with the ICO. The prosecution mentioned a number of aggravating factors, namely that:

- Data had been collected for commercial gain;
- Substantial profits had been made;
- Clifford had involved others in his offending;
- The offences had been committed in running of a business.

During the hearing at Kingston Magistrates' Court in December 2006, Clifford's defence barrister reminded the bench that his client had pleaded guilty at the first opportunity and that most of his work was 'completely lawful'. He also stated that a lot of Clifford's work was from Invex, a company run by a former police officer, and that his client felt pressured into taking on illegal work. Although the work was 'unlawful' and 'regrettable', it should be noted that the 'boundaries between what was illegal and what was legal became blurred'.[57]

The magistrate, Judith Hopkins, in sentencing Clifford stated that his offences were 'very serious' and 'systematic and planned'. Consequently, the defendant was sentenced to an 18 month community order including 150 hours unpaid work per offence. In addition he was ordered to pay a contribution to prosecution costs of £2000 within 6 months. After the case, Taylor declared that he was 'pleased' with the verdict[58]. Nevertheless, according to one correspondent present at the hearing, Hopkins 'hinted that the court would have considered sending [Clifford] to prison if the law had allowed it'.[59]

The Clifford verdict followed another high profile case, that of Sharon and Stephen Anderson. The Andersons, who traded as Analysis and Business Research, made £140,000 a year selling personal data.[60] They were convicted in November 2006, pleading guilty to 25 offences of obtaining and selling personal information unlawfully and asking for another 97 to be taken

into consideration. In addition, they were fined a total of £7,500. Taken with the recommendations in *What Price Privacy?*, this activity demonstrates the ICO's intention to target the growth in the illegal in personal data. Moreover, with the prominent law firms and retailers being among the ultimate recipients of the information 'blagged' by Clifford and the Andersons, the ICO have extended their investigations to include organisations who purchase this data.[61]

In this policy area, the ICO is taking a lead. If the DPA 1998 is amended, the UK will become one of the very few countries where custodial sentences are written into the primary data protection or privacy legislation. As a comparison, New Zealand, whilst particularly active in encouraging data protection compliance via tools such as Privacy Impact Assessments – discussed later in this paper - does not have a custodial option in its Privacy Act for this type of offence. Instead, prosecutions of that nature are usually made under the Crimes Act 1961 or the Summary Offences Act 1981.[62]

Follow-up report

The ICO's follow-up report, *What Price Privacy Now?* was published in December 2006.[63] The document reviewed progress over the previous seven months and detailed responses from the organisations identified as having a role to play in reducing demand for illegally acquired personal data and in raising awareness of the problem. Although a majority supported the ICO's proposals, the Commissioner found a few responses discouraging. For example, some media bodies, such as the BBC, failed to unequivocally condemn section 55 offences and were suspicious that the ICO's proposals could deter journalists from pursuing stories that were in the public interest. In response, the Commissioner stated that he was:

> '…not proposing the introduction of any new criminal offences and that there exist[ed] a defence in the Act for anyone acting in the public interest.'[64]

In addition, a table was published disclosing media publications identified from Operation Motorman, the number of transactions each publication had been involved in, and 'how many of their journalists (or clients acting on their behalf)' had used their services. A total of 31 publications were listed including tabloids, broadsheets and magazines. The ICO concluded the report by stating their commitment to continue to raise awareness and work with any organisation that wants to raise standards or produce clear guidance on their data protection obligations.[65]

6. Towards a balanced 'privacy toolbox'?

The threat of custodial sentences, although a powerful deterrent, is not the only compliance tool available. In a nod towards the work of Bennett and Raab, the Information Commissioner has promoted a mixed approach to the regulation of privacy.

In the last decade, this has been evidenced through the development of codes of practice for CCTV and employment practices, good practice notes and the regulator's support of European Commission model clauses for personal data transferred outside of the European Economic Area.

In *What Price Privacy?*, it is clear that this work has been extended. The report refers to joint working protocols with the Department for Work and Pensions (DWP), HM Revenue and Customs (HMRC), British Telecom and police forces around the country. Whenever DWP or HMRC staff identify suspect calls, a bogus call report is completed. The reports are collated and analysed, and when patterns are identified the cases are passed to the Information Commissioner for investigation.[66] Moreover, the ICO's Investigations Unit liaises almost weekly with police forces, 'often at their request for advice'.[67] Cooperation with the police has been enhanced through the decision of the Association of Chief Police Officers (ACPO) to include unauthorised disclosures of personal data in the annual risk assessment carried out by the police service and the Serious and Organised Crime Agency. Finally, ACPO have included confidentiality in a code of professional standards that is currently in development.[68]

Privacy Impact Assessments (PIAs)

In assessing risk of privacy abuses another tool, the PIA, has been increasingly promoted by the ICO, especially in relation to the proposed NIR.[69] PIAs gained currency in the 1990s as governments and businesses came to terms with the introduction of new information systems and the convergence of existing technologies. They are seen as a systematic risk assessment tool that can be usefully integrated into decision-making processes.[70] As such, the application of PIAs could reduce the risk of data being traded illegally. The New Zealand Privacy Commissioner, whose office has been active in the promotion of PIAs, defined the tool as:

> A systematic process that evaluates a proposal in terms of its impact upon privacy.[71]

In the US, where PIAs have been mandated for new federal-level public sector projects by the e-Government Act 2002[72], they have been defined by the Department of Justice as:

> …an analysis of how information in identifiable form is collected, stored, protected, shared, and managed in an IT system or online collection.[73]

The application of the technique varies. Some of the most detailed practical guidance has been issued by the New Zealand Privacy Commissioner.[74] PIAs are generally seen as an anticipatory instrument, to be ideally included at the 'concept definition stage' of systems development. In practice, it is a tool that can be used by private and public sectors, in particular for medium to large businesses and government agencies. The assessment can be undertaken

internally, providing the assessor has 'sound analytical and writing skills' and there is 'some external or independent oversight'.[75] Projects warranting a PIA can vary from obvious candidates such as the components of the proposed NIR to other mundane but significant projects for example merging internal business databases to enable new forms of client profiling or centralising a multi-national company's employee records in the UK. According to the New Zealand Privacy Commissioner, a typical PIA should include:

- Description of the project and information flows;
- The privacy analysis:
    - Collecting and obtaining information;
    - Use, disclosure and retention of information.
- Privacy risk assessment;
- Privacy enhancing responses;
- Compliance mechanisms.[76]

Yet, in spite of guidance and activity overseas, adoption of PIAs in the UK has been extremely slow. Although the Performance and Innovation Unit recommended their use in a report published in 2002,[77] there has been little progress since that date. In 2006, the case was further stated by the authors of the ICO-commissioned *A Report on the Surveillance Society*.[78] At the same time, the ICO expressed its intention to support work on PIAs, seeing it as 'still desirable'.[79]

Such work would be timely, and could dovetail with the regulator's current campaign against the illegal trade in personal data. Although a PIA feasibility study has been conducted in relation to social care provision in Scotland,[80] there is scope for further work in other policy areas. A particularly strong case can be made for the criminal justice sector, given the number of emerging and consolidated databases currently overseen by the Home Office and the police.[81] There are also overseas precedents in this sector, with PIAs being used by the United States in relation to Department of Justice / FBI databases, and in Hong Kong with regard to a 'new generation' national identity card scheme.[82] Although there has been uncertainty in the United States about whether PIAs can comprehensively address the privacy implications of authentication systems at federal level,[83] PIAs can usefully provide a 'macro level' look at privacy issues in e-government and business contexts.

7. Conclusions

The report on the illegal trade in personal data and campaigning for the introduction of custodial sentences is indicative of the more 'interventionist' stance being taken by the ICO, asserting greater influence over legislation and policy-making. In this respect, it has been seen that the ICO is ahead of other national data protection regulators. However, increased sentencing powers cannot alone be regarded as a panacea. Their value as a deterrent is difficult to predict, although the ICO argue that a number of central government departments, and the police, support a much tougher approach to

punishing those involved with illegal disclosure.[84] This new approach will require monitoring and regular review – by the Information Commissioner and independently - to measure its impact.

At the same time, greater compliance with the DPA 1998 also needs to be encouraged in order to ensure that new information systems are developed in privacy friendly ways. Greater attention has to be paid to the assessment of risk. In this paper, the adoption of PIAs – pioneered in New Zealand, mandated in the US and Canada – has been suggested as part of the solution. In May 2007 the Information Commissioner, in evidence submitted to a Home Affairs Committee Inquiry, placed renewed emphasis on PIAs.[85] The effectiveness of such a tool, and how it balances with more punitive measures designed to deter breaches of data protection principles, would also benefit from a comprehensive evaluation.

Acknowledgements

The author wishes to acknowledge the invaluable contribution made by Philip Taylor, prosecuting solicitor for the ICO, particularly in arranging attendance of the hearing at Kingston Magistrates' Court in December 2006 and commenting on an earlier draft of this paper. Clearly, he is not responsible for any ensuing errors or misinterpretations. Opinions expressed in this paper belong to the author. Finally, the author also wishes to state his gratitude to Dr Russell for his interest in this topic and to the anonymous referees for the constructive comments received.

Notes and References

[All links accessed on 13 February 2007.]

[1] ICO *What Price Privacy?* The Stationery Office, London, 10 May 2006.

[2] Ibid.

[3] DCA. *Increasing penalties for deliberate and wilful misuse of personal data. Response to consultation*. DCA, London, 7 February 2007.

[4] C J Bennett and C D Raab. *The governance of privacy: policy instruments in global perspective* (2nd edition), The MIT Press, Cambridge, Massachusetts, 2006.

[5] ICO, op cit, note 1, p 7.

[6] Home Office. *Strategic action plan for the national identity card scheme: safeguarding your identity*, COI, London, December 2006.

- According to this document, there will not be a single 'database' or 'system'. Instead, the National Identity Register is to initially comprise information from three existing databases: the Department of Work and Pensions' Customer Information System, existing biometric systems for asylum seekers and biometric visas and existing Identity and Passport Service systems.

[7] Number 10. Policy Review. Impact of data-sharing and privacy laws on customer service, 15 January 2007, http://www.number10.gov.uk/output/Page10759.asp; and N Morris. Big Brother: what it really means in Britain today, *The Independent*, 15 January 2007.

[8] ICO. *What Price Privacy Now?* The Stationery Office, London, 13 December 2006.

[9] *ICO v Clifford*, Kingston Magistrates Court, 12 December 2006.

[10] This interdependence could lead to a 'race to the top', where countries fashion their data protection policies according to the highest possible standard, or a 'race to the bottom' where countries might consider that a less regulated climate would attract global businesses wishing to bypass higher standards elsewhere. Refer:

- Bennett and Raab, op cit , note 4, xv.

[11] Bennett and Raab, op cit , note 4, xxv.

[12] J-P Bergfeld The impact of the EC Data Protection Directive on Dutch Data Protection Law, *Journal of Information, Law and Technology*, 1 (1), 1996 http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1996_1/bergfeld/

[13] Royal Philips Electronics. How Philips uses a Privacy Impact Assessment as a building block for the privacy compliance of its global IT systems, *Privacy Laws and Business annual conference*, 2005.

[14] Refer:

- C D Raab. The future of privacy protection, *Cyber Trust and Crime Prevention Project*, Office of Science and Technology, London, June 2004;
- Canada. Ontario. Office of the Information and Privacy Commissioner and Netherlands Registratiekamer, *Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector*, Information and Privacy Commissioner and Registratiekamer, Toronto,
- Canada. Ontario. Office of the Information and Privacy Commissioner and Netherlands Registratiekamer, *Privacy-Enhancing Technologies: The Path to Anonymity*, Information and Privacy Commissioner and Registratiekamer, Toronto, 2005.

[15] *Data Protection Act*, section 51(3), 1998.

[16] Refer:

- House of Commons. *Home Affairs Committee on Identity Cards*, 3 February 2004;
- ICO. *The Identity Cards Bill – the Information Commissioner's concerns*, June 2005. http://www.ico.gov.uk/eventual.aspx?id=2655;
- D Murakami Wood (ed). *A Report on the Surveillance Society*. *For the Information Commissioner by the Surveillance Studies Network*. September 2006.

[17] Cabinet Office. *Modernising Government*, Cm 4310, The Stationery Office, London, 1999.

[18] Cabinet Office. Performance and Innovation Unit. *Privacy and data-sharing: the way forward for public services*, April 2002.

[19] Cabinet Office. *Transformational government: enabled by technology*. Cm 6683, Cabinet Office, London, 2005.

[20] Ibid., pp 18-19.

[21] NHS Connecting for Health. A guide to the national programme for information technology, 2005.

[22] For a brief discussion of some of the problems that have, and continue to, beset Connecting for Health, refer:

- D Leigh and R Evans. Most patients reject NHS database in poll, *The Guardian*, 30 November 2006 http://www.guardian.co.uk/uk_news/story/0,,1960170,00.html
- T Collins. Supplier sets out risks facing NHS IT plan, *ComputerWeekly.com,* 13 February 2007 http://www.computerweekly.com/Articles/2007/02/13/221746/supplier-sets-out-risks-facing-nhs-it-plan.htm

[23] Every Child Matters. Factsheet - Information sharing index, 2006 http://www.everychildmatters.gov.uk/deliveringservices/index/

[24] Foundation for Information Policy Research (FIPR). *Children's databases – safety and privacy. a report for the Information Commissioner*, FIPR, 2006.

[25] J B Rule. *Private lives and public surveillance*, Allen Lane, London, 1973, p 309.

[26] The systems are: the Department of Work and Pensions' (DWP) Customer Information Service, which holds national insurance records; the Identity and Passport Service computer system; and, initially, the existing biometric system used for asylum seekers. Refer:

- Home Office. Strategic Action Plan for the National Identity Scheme: Safeguarding your identity, COI, London, 2006, pp 10-11.

[27] BBC News. Giant ID computer plan scrapped, *BBC Online*, 19 December 2006. http://news.bbc.co.uk/1/hi/uk_politics/6192419.stm

[28] BBC News. Tesco 'spychips' anger customers, *BBC Online*, 26 January 2005. http://news.bbc.co.uk/1/hi/business/4209545.stm

[29] PWC. *Information security breaches survey: technical report*. Published for the DTI, April 2006. http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf

[30] Ibid., p 4.

[31] K Zetter. Hackers clone e-passports, *Wired.com*, 3 August 2006. http://www.wired.com/news/technology/1,71521-2.html

[32] The author is particularly grateful to Mr Taylor for his help in confirming the order of events in this section.

[33] ICO, op cit, note 1, p 15.

[34] The Metropolitan Police later launched Operation Glade into possible corruption by police officers or civilian police officers:
- ICO, op cit, note 1, p 15.

[35] ICO, op cit, note 1, p 17.

[36] The defendant was understood to have been suffering a terminal illness. Telephone conversation with Philip Taylor, 29 June 2006.

[37] Between mid-November 2002 and January 2006, the ICO brought 25 section 55 prosecutions in Crown and Magistrates Courts in England and Wales. Convictions were obtained in all but three of the cases. Refer:
- ICO, op cit, note 1, p 12.

[38] ICO, op cit, note 1, p 27.

[39] For example, refer:
- BBC News. Privacy traders 'must be jailed', *BBC Online*, 12 May 2006. http://news.bbc.co.uk/1/hi/uk_politics/4762937.stm
- Dowell, B. Journalists 'face conviction' over data breaches, *The Guardian*, 12 May 2006. http://www.guardian.co.uk/uk_news/story/0,,1773798,00.html

[40] ICO, op cit, note 1, p 5.

[41] A statutory body established under the Private Security Industry Act 2001 to introduce compulsory licensing for private investigation firms.

[42] The industry body for private investigators: http://www.theabi.org.uk/

[43] ICO, op cit, note 1, pp 5-6.

[44] Ibid., 16.

[45] Ibid., 31.

[46] The questions asked the institutions for information on: the steps they would take to publicise the report among their members; their willingness to condemn unequivocally section 55 offences; changes – to be made or proposed, within the next six months – to disciplinary rules, codes of practice and other instruments with the aim of 'improving [their] control or influence over the illegal buying and selling of personal information'. Ibid., 33-4.

[47] Telephone conversation with Philip Taylor, 29 June 2006.

[48] The Guardian. Leader. Bugs in the system, *The Guardian*, 12 August 2006. http://www.guardian.co.uk/commentisfree/story/0,,1842910,00.html

[49] C Tryhorn. Clive Goodman sentenced to four months. *The Guardian*, 26 January 2007. http://www.guardian.co.uk/uk_news/story/0,,1999276,00.html

[50] Ibid.

[51] DCA. *Increasing penalties for deliberate and wilful misuse of personal data. Consultation.* 24 July – 30 October 2006. http://www.dca.gov.uk/consult/misuse_data/cp0906.htm

[52] Ibid., pp 5-6.

[53] Ibid., p 10.

[54] Ibid., p 13.

[55] DCA, op cit, note 3.

[56] ICO. *Information Commissioner v Anthony Gerald Clifford. Draft Opening*. November 2006. [Unpublished].

[57] Author's notes from court hearing, 12 December 2006.

[58] Ibid.

[59] J Rozenberg. Blagger's guide to cheating the system, *The Telegraph*, 14 December 2006. http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/12/14/nlaw14.xml

[60] D Leigh and R Evans Illegal investigators, a detective agency, and a leading law firm, *The Guardian*, 15 November 2006. http://www.guardian.co.uk/crime/article/0,,1947915,00.html

[61] Ibid.

[62] New Zealand. Email correspondence with Office of the Privacy Commissioner, 10 January 2007.

[63] ICO, op cit, note 8.

[64] ICO, op cit, note 8, p 21.

[65] ICO, op cit, note 8, p 28.

[66] ICO, op cit, note 1, pp 12-13.

[67] ICO, op cit, note 1, p 13.

[68] ICO., op cit, note 8, p 26.

[69] Refer:
- House of Commons, op cit, note 16;
- ICO, op cit, note 16.

[70] R Clarke. *A history of Privacy Impact Assessments*, February 2004. http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist.html

[71] New Zealand. Privacy Commissioner, *Privacy Impact Assessment Handbook*, March 2002. http://www.foi.gov.uk/sharing/toolkit/pia_h-book.pdf

[72] PIAs have also been mandated in Canada. Refer:
- Canada. Treasury Board Secretariat, *Privacy Impact Assessment Policy*, 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp

[73] United States. Department of Justice. Office of the Deputy Attorney General, *Privacy Impact Assessments: Official Guidance*, revised 7 August 2006. http://149.101.1.32/pclo/pia_manual.pdf

[74] New Zealand, op cit, note 71.

[75] New Zealand, op cit, note 71, p 14.

[76] New Zealand, op cit, note 71, p 21.

[77] Cabinet Office, op cit, note 18.

[78] Murakami Wood, op cit, note 16, pp 76-7, 81, 89-95.

[79] ICO. *Minutes of Policy Committee*, 18 September 2006. http://www.ico.gov.uk/Home/about_us/who_we_are/corporate_information/policy_committee.aspx

[80] C D Raab, C., P 6, A Birch, and M Copping. *Information sharing for children at risk: impacts on privacy*, e-Care Programme, Leith, Health Department, Scottish Executive. Publication: 23357, 2004.

[81] In addition to the NIR, these systems include a number of police databases such as the Facial Images National Database, IDENT1 (fingerprints), Lantern (hand-held fingerprint ID) and ViSOR (violent and sex offenders).

[82] Hong Kong. Security Bureau. *HKSAR Identity Project – Initial Privacy Impact Assessment Report*, 2001. http://www.legco.gov.hk/yr00-01/english/panels/se/papers/b715e01.pdf

[83] S H Holden and L I Millett. Authentication, privacy and federal e-government, *The Information Society*, 21, 367-77, 2006.

[84] ICO, op cit, note 1, p 26.

[85] The Information provided evidence to the Home Affairs Committee Inquiry into 'The Surveillance Society' on 1 May 2007. Refer:
- ICO. *Information Commissioner calls for new privacy safeguards to protect against the surveillance society*, 1 May 2007. http://www.ico.gov.uk/upload/documents/pressreleases/2007/surveillance_society_follow_up001.pdf

For further details of the Commissioner's evidence, refer:
- ICO. *Home Affairs Committee Inquiry into 'The Surveillance Society?' Evidence submitted by the Information Commissioner*, 23 April 2007. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/home_affairs_committee_inquiry_into_surveillance_society.pdf