Legal update

Data protection: Tougher enforcement and increased power for the Information Commissioner?

Ewan Nettleton
is a Senior Associate Solicitor in the Intellectual Property Department at Bristows. He specialises in Intellectual Property Law, with an emphasis on litigation. He has an MA in Chemistry and a D Phil in Protein Chemistry and is particularly interested in matters relating to the IT and pharmaceutical industries.

Ian Turner
is a Trainee Solicitor at Bristows. He has a BSc and a PhD in Biochemistry.

Keywords *Data protection, enforcement, Information Commissioner, power, breach, HMRC*

Abstract Database marketers, more than most, should be aware of their obligations as regards protection of data and the role of the Information Commissioner's Office. The perception of those who hold personal data, so-called 'data controllers' under the Data Protection Act, has been affected by headline news in the past year or so. Various committees and independent reviews are investigating the relevant legal provisions in light of recent breaches of data security and in particular HMRC's loss of data, reportedly comprising the banking details of 25 million recipients of child benefit. Here we assess the various calls for changes to the law and what tightening of the rules might mean for database marketers.

Journal of Database Marketing & Customer Strategy Management (2008) **15,** 207–212.
doi:10.1057/dbm.2008.9; published online 25 August 2008

DRIVING FORCE FOR CHANGE

On 20th November, 2007, the Chancellor of the Exchequer, Alastair Darling, announced in the Commons that HMRC had lost two computer discs reportedly containing the personal details of all families in the UK with a child under 16, some 25 million individuals and 7.25 million families receiving child benefit.[1] The data included names, addresses, dates of birth and in some cases bank account details. Unfortunately, this has not been an isolated incident, with many cases of loss of data and breaches of the data protection requirements being uncovered in the private and public sectors since that time. Indeed, the announcement of the HMRC loss was closely followed by a finding from the Information Commissioner's Office (ICO) that the Foreign Office had breached the Data Protection Act,[2] and since the HMRC announcement, the ICO has been notified of almost 100 data breaches (62 in the public sector and 28 in the private sector).[3] Most recently, enforcement action has been taken against Marks & Spencer following unencrypted personal information of 26,000 employees being lost when a laptop was

Ewan Nettleton
Bristows
100 Victoria Embankment,
London EC4Y 0DH, UK
Tel: 020 7400 8000;
Fax: 020 7400 8050;
email: ewan.nettleton@bristows.com

stolen from a contractor's house.[4] This has led to Marks & Spencer being required to encrypt all such data by April 2008.

Perhaps unsurprisingly in these circumstances, there have been calls from numerous sources for a tightening up of data protection law and for more powers for the ICO. This paper considers some of the assessments being made and the changes proposed, and seeks to evaluate the likely long-term effects for data controllers such as database marketers.

DATA PROTECTION AND THE ICO'S POWERS — A BRIEF REMINDER

The Data Protection 1998 Act, which implemented EU-wide legislation on the protection of personal data, gives individuals rights, such as the right to ascertain what information is held about them, and imposes obligations on data controllers to ensure that personal data is processed properly.[5] These data protection rules, coupled with the rules relating to unsolicited marketing communications set out in the UK's Privacy and Electronic Communications Regulations,[6] are the principal rules with which the ICO will expect database marketers to comply.

SUMMARY OF THE ONGOING REVIEWS

Coincidentally, in October 2007, just before the HMRC announcement, the Prime Minister had asked the Information Commissioner, Richard Thomas, and the Director of the Wellcome Trust, Mark Walport, to conduct an independent review of the framework for the use of information in the private and public sectors. This 'Data Sharing Review' was to provide recommendations on changes to the law and how policy should be developed to ensure accountability. In December 2007, Mr Thomas and Dr Walport launched a consultation on these issues, which closed in February 2008. Notably, even before the review began, the ICO had been widely reported as interested in broadening its powers in relation to the UK's data protection regime. We therefore anticipate that when the report is released later this year, a number of changes bolstering the regime and the ICO's powers will be recommended.

Additionally, following the announcement of the HMRC data loss, two further reviews were announced. The first was specifically aimed at discovering exactly what went wrong at the HMRC and is being conducted by Kieran Poynter, the Chairman of PricewaterhouseCoopers LLP. The second is a wider review of data handling procedures in government by the Cabinet Office and is headed up by Robert Hannigan, the Head of Intelligence, Security and Resilience at the Cabinet Office. Mr Hannigan is considering the procedures in the government's departments and agencies for the protection of data, their consistency with current government-wide policies and standards, and the arrangements for ensuring that procedures are being fully and properly implemented. Notably, part of the review process is to look at improving standards and procedures, including the introduction of better compliance and audit arrangements.

Both Mr Poynter and Mr Hannigan have issued interim reports in relation to their reviews,[7,8] and their full reports are expected later this year. Both have made general recommendations and reported positive developments, which are already in process, but all too often these seem to be only recommendations of best practice advice already available from other sources. That said, more concrete recommendations for changes to the law are proposed in the Cabinet Office's interim review (as discussed further below), suggesting that Robert Hannigan's review, when issued in full, may contain more substantive recommendations.

The subject of data protection has also been considered by the House of Commons' Justice Committee, The Joint

Committee on Human Rights and the House of Lords Science and Technology Committee, all of which have made recommendations recently. Each tends to repeat similar recommendations for changes to the Data Protection Act, and these are discussed further below.

PROPOSED CHANGES TO THE LAW

In December 2007, the ICO published what amounts to a shopping list of changes it would like to see made to the Data Protection Act 1998, and its views on why these changes need to be made.[9] The ICO's principal recommendations are that the following powers and penalties should be created:

- a penalty for knowingly or recklessly failing to comply with the data protection principles so as to create a substantial risk that damage or distress will be caused to any person;
- a power for the Information Commissioner to inspect personal data and the circumstances surrounding its processing in order to assess whether or not any processing of the data is carried out in compliance with the Act;
- a power for the Information Commissioner to require a data controller to provide him with a report by a skilled person;
- enhanced enforcement powers to enable the Information Commissioner to bring seriously unlawful processing to an immediate halt, to place formal undertakings on a statutory basis and to enable the Information Commissioner to take enforcement action to prevent breaches of the Data Protection Act that are likely to occur; and
- information notices that can be served on any person rather than just a data controller.

Noting that, in its view, there is '*a shortfall in the sanctions available… and the means of enforcing those sanctions swiftly and effectively*', the ICO makes the case for each of these changes. In doing so, the ICO points to various practical examples, not least the HMRC data loss where it observes that, even if the enquiry being undertaken by Mr Poynter were to find that HMRC had acted knowingly or recklessly in allowing an unprecedented security breach to take place, the Information Commissioner would have no powers to impose any penalty. These proposals are in many cases supported by the various other reviews and committees referred to above, as summarised below.

One of the ICO's recommendations, giving the Information Commissioner the power to inspect personal data and the circumstances surrounding its processing, is in effect a right to audit data controllers in order to assess whether there have been any breaches of the Data Protection Act. As explained in a previous paper,[10] a right of audit has long been notable in its absence from the ICO's armoury. On 21st November, 2007, the Prime Minister, however, stated at Prime Minister's Questions:

> 'We will give the Information Commissioner the power to spot-check Departments, to do everything in his power and our power to secure the protection of data. In other words, we will do everything in our power to make sure that data are safe'.[11]

This has been welcomed by the ICO as this is the sort of power that has been repeatedly called for.

While the Prime Minister's statement appears to have been made in relation to government departments, it is notable that The Cabinet Office's interim report recommended that the power to '*spot-check*' be extended from central government to the entire public sector.[12] Furthermore, the Information Commissioner has publicly called for this audit power to cover all organisations, which would bring private organisations within its remit.[13] It therefore

seems likely that should the Government seek to change the legislation, the audit power would be extended to the public and private sectors, even though the issue of data security has perhaps been brought into focus most recently by issues of data handling in the public sector.

The number of voices calling for a requirement to report data handling breaches makes this another likely addition to the Data Protection Act should legislative changes be tabled by the government. In the words of the ICO, '*consideration should be given to security breach notification obligations in the UK. These are used in other jurisdictions and involve the organisation which is the subject of a breach being obliged to tell those individuals affected by it such as those whose personal information is involved, as well as, in some cases, the regulator*'.[14] One difficulty with such legislation is defining the requirement to report, so as not to require every single minor matter to be reported,[15] which would make the system, practically speaking, unworkable. Any draft legislation would require careful scrutiny to ensure that an unworkable requirement is not introduced into the data protection legislation.

It is, however, notable that in the US around 40 States have enacted laws requiring companies to notify consumers whose personal information has been compromised,[16] and various bills that could lead to Federal US legislation requiring notification are currently before Congress.[17] Furthermore, in the EU, the European Commission has put forward a proposal that would require mandatory notification of security breaches resulting in users' personal data being lost or compromised.[18] So, notwithstanding the difficulties, concrete efforts are being made to put such a law in place.

A recent report on data protection and human rights by the Joint Committee on Human Rights[19] included evidence from the Minister of State at the Ministry of Justice, Michael Wills MP, who is responsible for (among other things) data protection. Readers may be unaware that a Minister with such responsibility existed. Indeed, there may well be a lack of awareness generally, given that Mr Wills only heard of the HMRC's data loss when the news was announced by the Chancellor in the House of Commons.[20] The report has, however, recommended an enhancement of the role of the Data Protection Minister to champion data protection and provide policy guidance, in addition to overseeing the data protection legislation. It seems likely that this role would remain principally within the public sector, but the private sector should be aware of the possible overlap with the messages coming from the ICO.

In addition to these measures seeking to improve the scrutiny of data handling, there were also two proposals for changes to the penalties for breaching the data protection rules. These have now been introduced in the Criminal Justice and Immigration Act 2008, which received royal assent on 8th May. First, an amendment proposed in the House of Lords to the Bill that led to this Act provides a mechanism for increasing the penalties available under Section 55 of the Data Protection Act.[21] The amendment confers on the Secretary of State the power to make an order altering the maximum penalty for an offence under Section 55, and the maximum penalty could be altered in this way up to a maximum of two years' imprisonment for a conviction on indictment.[22] Such a provision was supported because the provision is used to prosecute individuals involved in the black market for personal information.

The second of the changes is perhaps more controversial. It has been the ICO's desire to introduce a new offence that would enable the prosecution of those data controllers who recklessly or repeatedly allow significant data breaches. This would provide a much more powerful enforcement tool to the ICO, because

currently a two-stage enforcement approach must be adopted, and data controllers can only be subject to criminal proceedings for breach of an enforcement notice. The House of Lords in its third reading of the Bill tabled an amendment to create a new criminal offence. The House of Commons opposed this, but the government, giving in to considerable cross-party pressure, tabled its own amendment in lieu of the House of Lords criminal sanction. This was accepted and is part of the new Criminal Justice and Immigration Act.

The new Section 55A of the Data Protection Act as inserted by the Criminal Justice and Immigration Act creates a power for the Information Commissioner to impose a monetary penalty. The new section allows a penalty notice to be served upon a data controller if the Commissioner is satisfied that there has been a serious breach of the duty to comply with the data protection principles (Section 4(4)) when the following additional criteria are satisfied:

— the breach was of a kind likely to cause substantial damage or distress; *and*
— the breach was deliberate; *or*
— the data controller knew or ought to have known
  - there was a risk that the breach would occur; and
  - that the breach would be of a kind likely to cause substantial damage or distress; but
  - failed to take reasonable steps to prevent the breach.

The new Section 55A leaves open the maximum level of the fines and this will be set by secondary legislation at a later date. Under the new Section 55B, the Information Commissioner must serve the data controller with a notice of intent before serving such a penalty notice, and the new Section 55C requires the ICO to produce guidance on the operation of these provisions, which is to be approved by the Secretary of State and both Houses of Parliament. It will thus be some time before the true scope of the new power is clear.

The introduction of this quasi-criminal enforcement mechanism is fairly controversial. Indeed, in the parliamentary debates, reservations were expressed about the ICO acting as policeman, judge and jury over data controllers. The new Section 55B, however, provides some comfort by setting out the procedural rights both before and after the serving of a monetary penalty notice. The ICO must first serve the notice of intent, which allows a certain period of time for the data controller to make written representations before a penalty notice can be issued. There is also a right of appeal against both the issue of a penalty notice and the amount of a penalty notice.

CONCLUSIONS

Recent high profile losses of large quantities of personal data by public sector institutions, such as HMRC in particular, have affected the perception of data controllers in general and have led to calls from many quarters for an enhancement of the UK's data protection requirements and enforcement provisions. Calls for enhanced powers for the ICO from both the Information Commissioner himself and from a number of heavyweight committees are likely to be acted upon, and this would tighten up the UK's data protection regime, with rights of audit to identify data breaches and requirements for such breaches to be communicated to affected individuals being one possible outcome. Additionally, changes to the sentences and offences for data protection breaches have already been made by the new Criminal Justice and Immigration Act and may significantly change the risks faced by data controllers, although the true scope of the new provisions is not yet clear. While the conduct of data controllers within the public sector may have triggered the calls

for these changes, individuals such as database marketers, working in the private sector, need to be aware of the changes made and being proposed, because they could apply to them.

References and Notes

1 See, for example, the BBC article '*UK's families put on fraud alert*' dated 20th November, 2007 available on the BBC website (http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm).
2 ICO press release '*Foreign office in breach of the Data Protection Act*', 13th November, 2007.
3 ICO press release '*Roll call of data breaches grows*', 22nd April, 2008.
4 ICO press release '*ICO takes enforcement action against Marks and Spencer*', 25th January, 2008.
5 For an overview of the data protection requirements on data controllers, see 'Don't bin your data protection responsibilities', *Journal of Database Marketing and Consumer Strategy Management*, Vol. 14, No. 4, pp. 311–314.
6 These rules have also been summarised in previous articles. See for example the following articles published in the *Journal of Database Marketing and Consumer Strategy Management*: '*Electronic marketing and the new anti-spam regulations*', Vol. 11, No. 3, pp. 235–240; '*Getting Tough on Spam*', Vol. 12, No. 4, pp. 357–361; and, '*Telephone Marketing Out in the Cold?*', Vol. 12, No. 2, pp. 172–176.
7 '*Data Handling Procedures in Government: Interim Progress Report*', Cabinet Office publication, December 2007 (available at http://www.cabinetoffice.gov.uk/reports/~/media/assets/www.cabinetoffice.gov.uk/publications/reports/data/data_handling%20pdf.ashx).
8 Letter from Kieran Poynter to Rt Hon Alistair Darling MP, 14th December, 2007 (available at http://www.hm-treasury.gov.uk/media/E/E/poynter_review171207.pdf).
9 '*Data Protection Powers and Penalties*', ICO publication of December 2007 (available at http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/data_protection_powers_penalties_v1_dec07.pdf).
10 See ref. 5 above.
11 See the First Report of the House of Commons Select Committee, on '*Protection of Private Data*', 3rd January, 2008 (available at http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf).
12 Para 44, '*Data Handling Procedures in Government: Interim Progress Report*', Cabinet Office publication, December 2007.
13 See for example 'Richard Thomas: Individuals value their privacy – institutions do not', *The Independent*, 27th November 2007 (http://www.independent.co.uk/opinion/commentators/richard-thomas-individuals-value-their-privacy--institutions-do-not-759001.html).
14 See the First Report of the House of Commons Select Committee, on '*Protection of Private Data*', 3rd January, 2008 (available at http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf) at para 19 which reports evidence submitted by the Information Commissioner to the Home Affairs Committee in its inquiry into '*A Surveillance Society?*'.
15 As recognised by the House of Lords Science and Technology Committee in paras 5.55–5.57 of their report on '*Personal Internet Security*', 10th August, 2007 (available at http://www.parliament.the-stationery-office.com/pa/ld200607/ldselect/ldsctech/165/165i.pdf).
16 See for example '*CSO Disclosure Series | Data Breach Notification Laws, State By State*' by Scott Berinato, 12th February, 2008 (available at http://www.csoonline.com/article/221322).
17 See for example '*Federal breach notification stuck in Congress*' by Zach Church, 1st May, 2008 (available at http://searchcio-midmarket.techtarget.com/news/article/0,289142,sid183_gci1309396,00.html).
18 EU Commission proposal for a Directive amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, 2007/0248 (COD), 13th November, 2007.
19 Report of the House of Lords and House of Commons Joint Committee on Human Rights on '*Data Protection and Human Rights*', 4th March, 2008.
20 See Para 23 of the report, *ibid*.
21 Section 55, Data Protection Act 1998 makes it an offence to disclose, obtain or procure the disclosure of confidential personal information knowingly or recklessly without the consent of the data controller.
22 See para 45 of the Explanatory Notes on the Lords' amendments to the Justice and Immigration Bill as brought from the House of Lords on 30th April, 2008 (available at http://www.publications.parliament.uk/pa/cm200708/cmbills/104/en/2008104en.pdf).