Legal Update

Taking stock of the UK's data retention requirements

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.

Eric Klotz

is a trainee solicitor at Bristows. He has a D Phil in Organic Chemistry.

ABSTRACT On the back of a recent extension of the UK's data retention requirements in April 2009, the Government has published the results of its consultation on *Protecting the Public in a Changing Communications Environment*. The consultation sought input from the public on proposals for further changes to the data retention obligations placed on companies that provide communications services. With growing concerns over the UK's *surveillance society* and high-profile policy initiatives that require storage of personal data such as the national DNA database and national identity cards, commentators are looking at the results of the consultation with great interest. This article digests the responses and the government's reaction to them in light of recent legislative changes, and seeks to assess the potential impact on database marketers and what the future may hold.

Journal of Database Marketing & Customer Strategy Management (2010) 17, 59–65. doi:10.1057/dbm.2009.33

Keywords: data retention; consultation; government; legislation

INTRODUCTION

Over the past decade, governments around the world have introduced laws requiring communication service providers to retain certain data in the course of communication exchanges. These requirements have been put in place to protect citizens from terrorism and organised crime, and they form part of a general trend towards the bolstering of surveillance powers. The requirements imposed will have an effect on users of communications services, including database marketing companies, because their data will have to be retained,

and meeting the data retention requirements comes at a price that ultimately may be passed on to them.

In 2007, the UK Government passed legislation¹ requiring public authorities to retain certain communications data for 12 months. As regular readers of the *Journal* may recall,^{2,3} the 2007 Regulations were brought in to implement the provisions of a European Directive on Data Retention.⁴ The data retention requirements under this Directive initially related only to telephone data, with Member States able to postpone the

Correspondence:
Ewan Nettleton
Bristows, 100 Victoria
Embankment, London,
EC4Y 0DH, UK
E-mail: ewan.nettleton@
bristows.com

implementation of the provisions in the more tricky area of Internet and email data until March 2009. The 2007 Regulations therefore only required retention of data from fixed and mobile telephony communications.

The 2007 Regulations left companies with uncertainties over the types of data to which they applied, and also about the extent to which the cost to companies in meeting the requirements would be reimbursed. To complicate matters still further, there was a separate voluntary regime that included provisions relating to Internet data. These required certain Internet information to be held for 6 months (in addition to a 12-month requirement for telephony data that was consistent with the 2007 Regulations).⁵ The type of Internet data that needed to be retained under this voluntary code included email data (including from/to email addresses, and date and time sent) and Internet Service Provider data.

In April 2009, new Regulations were brought in to the United Kingdom⁶ to extend the legislative data retention requirements to Internet communications data as required by the Directive. This, however, seems unlikely to be the end of the matter. The UK Government has proposed further extensions to the state's surveillance powers relating to communication data, on which it sought input by way of a public consultation published in April 2009.⁷ This article provides an update on the recent legislative developments and considers the summary of responses to the Government's recent consultation.

THE 2009 REGULATIONS

Following an earlier consultation, the Data Retention (EC Directive) Regulations 2009 came into force on 6 April 2009, replacing the 2007 Regulations we described previously.⁴ Like the 2007 legislation, the 2009 Regulations apply to public

communications providers, including providers of public electronic communications networks and public electronic communications services. The term is therefore defined broadly and will include most communications companies. The retention period specified is still 12 months, but the key difference compared with the 2007 Regulations is the extension of the data retention requirements to Internet and email data.

The requirements vary a little depending on the type of data covered, but broadly speaking the 2009 Regulations require public communications providers to retain the data necessary for the following:

- tracing and identifying the source of a communication;
- identifying the destination of a communication;
- identifying the date, time and duration of a communication;
- identifying the type of communication; and, in some cases,
- identifying users' communication equipment (or what purports to be their equipment) and the location of mobile communication equipment.

Importantly, while the data include information such as the Internet protocol address and time of communications, they do not cover the content of the communications themselves, and are concerned with tracing and identifying communications and the persons involved. Nevertheless, the changes represent a considerable addition to the burden on public communications providers, with a major increase in the data they must now retain.

This leads to a further important aspect of the 2009 Regulations, namely who bears the cost of these increased data retention requirements. Perhaps not surprisingly, the 2009 legislation adopts the same approach as the 2007 Regulations, with

communication service providers being required to enter into agreements with the authorities in advance for the reimbursement of their costs. The wording used is similar in the 2009 Regulations providing that the Secretary of State *may* reimburse any expenses incurred by a public communications provider in complying with the provisions of these Regulations. This reimbursement may be subject to advance notification and agreement, and to auditing of the costs incurred.⁸

THE APRIL 2009 CONSULTATION

In addition to enacting the 2009 Regulations, the Government also released a consultation paper in April 2009 seeking input from the public on questions concerned with increasing the potential uses of communications data still further. The consultation document set out the Government's observations on the role communications data play in enabling law enforcement, security and intelligence agencies and the emergency services to protect the public; the challenges that ever more sophisticated technologies bring; and the options for meeting these challenges.

Of the options mentioned, the consultation paper stated that the Government had no plan to create a centralised database to store all such communications data. However, it suggested that doing nothing in the face of these challenges was not an option. Instead, the consultation document advocated a *middle way* that would seek to balance the rights to privacy and security. This, the Government suggested, would be based on the existing model of collecting and retaining data by communications service providers, and allowing them to be accessed on a case-by-case basis under the Regulation of Investigatory Powers Act

2000 (RIPA), which provides for public authorities to acquire such communications data.⁹

In light of these proposals, the Government sought input on the following questions in the consultation document:

1. *On the basis of the evidence and subject to current safeguards and oversight arrangements, do you agree that communications data is vital for law enforcement, security and intelligence agencies and emergency services in tackling serious crime, preventing terrorism and protecting the public?*
2. *Is it right for Government to maintain this capability by responding to the new communications environment?*
3. *Do you support the Government's approach to maintaining our capabilities? Which of the solutions should it adopt?*
4. *Do you believe that the safeguards outlined are sufficient for communications data in the future?*

THE SUMMARY OF RESPONSES

The summary document published by the Home Office provides both a summary of the responses received and some further insights into the Government's thinking on what is required in order to achieve its objectives. Of the 221 responses, 167 came from members of the public, while the other 54 were from organisations in the telecommunications industry, security agencies, Internet service providers and other public organisations. Notably, the summary suggests that 90 of the respondents did not address the questions asked, but objected generally to the consultation paper, mostly on the grounds of opposition in principle to any sort of surveillance. These seemingly negative responses are not included in the summary, and the percentages quoted (and referred to below) do not take them into account. The key points arising from the summary document published by the Home Office

are summarised in relation to each of the questions below.

Question 1 – Whether communications data is vital for law enforcement, security and intelligence agencies and emergency services in tackling serious crime, preventing terrorism and protecting the public

The summary suggests that 59 per cent of the respondents agreed that communications data are an important and in some cases vital tool for tackling crime and preventing terrorism, with 18 per cent disagreeing. Not surprisingly, the Government's position is that they provide a vital tool for these purposes. However, it acknowledges that the communications data should be retained by communications services providers and not by the Government, and should only be used if necessary and proportionate to do so, noting the need to be consistent with Article 8 of the European Convention on Human Rights (the right to respect for one's private and family life, and one's home and correspondence).

Question 2 – Whether Government should maintain this capability by responding to the new communications environment

Fifty-three per cent of respondents agreed that the government needed to respond to a changing communications environment, with a recognition of the challenges posed by rapidly changing technologies. The Government was also of this view, emphasising the need to develop the ability of public authorities to use communications data from a wider range of technologies in order to provide the same level of public protection as in the past. However, it pledged to ensure that use of communications data would continue to be proportionate and reasonable with proper accountability, safeguards and oversight.

Question 3 – Support for the Government's suggested approach

This question garnered less support from the respondents, with only 29 per cent supporting the Government's suggested approach, and this is without counting the other negative responses referred to above. Thirty-eight per cent of respondents expressed their opposition, with the majority suggesting the Government select the *do nothing* option and others suggesting that there should be more discrimination about which data are to be retained.

Not surprisingly, communications service providers also raised concerns about the costs of retaining large quantities of data, noting the importance of continuing the Government's compensation scheme for service providers for additional costs arising from the retention of communications data. They also raised concerns that additional retention requirements might not be reasonable or even technically feasible, and expressed worries that the proposals could lead to additional demands for disclosure of information to third parties, placing a further burden on companies. They argued that communications data should only be accessible to the authorities under the provisions of RIPA, and not through any other statutes or legal powers.

Notably, the Government expressed the view that the 2009 Regulations do not adequately maintain existing communications capabilities because the Regulations implemented the Data Retention Directive, whose aim was to harmonise the law in this area across European Member States. By way of example, the Government pointed out that the Regulations do not cover communications data relating to web chat or third-party service providers located outside the United Kingdom. Acknowledging that access to retained data through different statutory frameworks such as the Social Security Fraud Act 2001 may

be undesirable, the Government stated that it would carry out a review of all mechanisms by which public authorities can obtain the data to determine whether a single means of access via RIPA was practicable.

Brushing off the rather negative reaction to this question, the Government concluded by saying that it was confident that its proposed solution was technically feasible and that it would continue to work with communications service providers in its development.

Question 4 – Whether the safeguards outlined are sufficient for communications data in the future

There was also limited support for the safeguards outlined in the Consultation Document for communications data, with only 26 per cent of respondents believing them to be measured and proportionate. In the wake of many high-profile data losses from companies and government departments, it is hardly surprising that there was widespread concern about the safety and security of retained communications data and the potential for abuse. Fifty per cent felt that the safeguards were inadequate. Communications service providers considered that safeguards should continue to include statutory restrictions on who can access communications data, and to ensure that third-party communications data cannot be used for commercial purposes in an anti-competitive manner. They also raised concerns about how the requirements of the Data Protection Act 1998 would apply in the context of communications data, suggesting that this be made clearer.

The Government acknowledged that the use of communications data should be subject to a comprehensive range of safeguards, citing the restrictions under RIPA and the requirements of the Data Protection Act 1998 as safeguards that are

already in place. It also referred to its current moves to strengthen the powers of the data protection watchdog the Information Commissioner, and to introduce custodial sentences for certain offences under section 55 of the Data Protection Act 1998.¹⁰ While the Government agreed with the need for independent oversight of the way in which public authorities access communications data under RIPA, its summary document dismisses the suggestion that authorisation by magistrates be required in relation to all acquisition of communications data, suggesting that this could seriously impair effectiveness without any real benefits in terms of protecting privacy.

COMMENT

While the summary of responses includes little concrete detail on what steps will be taken, it concludes with a statement that the Government will continue to develop the approach it proposed in the consultation document with a view to bringing forward the necessary legislation. However, it would appear that the government has postponed its plans, at least in the short term, as there are no relevant legislative proposals in the current government legislative programme.

The Government's proposals have also suffered a knock from the Information Commissioners' Office, which published an article criticising them from a data retention perspective and suggesting that the case has not yet been fully made out for routine collection and retention of further communications data covering the entire population.¹¹ The article stated that the mere fact that communications data have proved useful in certain specific law enforcement cases does not mean that such surveillance would be useful or legitimate for the entire population on a *just in case* basis. Furthermore, it pointed out that surveillance under RIPA has been the subject of heated debate over inappropriate use, and that any legislation should not be

drafted overly broadly in a way that could allow misuse of the data. The Information Commissioner suggested that one option would be to target particular data, retaining a much narrower range of data.

Quite apart from the technical difficulties and issues over data protection, communications service providers highlighted the substantial cost implications in the consultation responses. A question asked in the House of Lords has provided insights into the actual costs involved,¹² with the Government stating that the amount paid out to telephone companies and Internet service providers to assist them in the voluntary retention of data in 2007 was over £8 million pounds.¹³ Clearly these are very significant costs, and it is hardly surprising that communications service providers want to ensure the reimbursement of such payments to prevent them (or their customers) from having to foot the bill. These figures, which represent only the amounts paid out and presumably not therefore the full costs to communications service providers, also highlight the economic toll of these measures, particularly with the extension of the requirements to Internet data earlier this year.

CONCLUSIONS

The Government has enacted legislation implementing the provisions of the Data Retention Directive, including, as of this year, requirements for the retention of Internet and email data. However, its recent consultation makes clear that the Government wants to go further in order to keep up with fast-moving technologies and threats posed to national security. The responses to the consultation are negative on the whole, with concerns raised about the Government's suggested approach and many favouring the *do nothing* option. While the lack of concrete proposals contained in the Government's summary of responses suggests that the implementation

of the Government's suggested approach is still some way off, the tone of the summary document implies that the issue is unlikely to go away.

Companies such as database marketers, whose businesses revolve around working with data, should watch these developments with interest, because the figures quoted for the costs to communications service providers were high even before the requirements were extended to the retention of Internet and email data. While the latest Regulations still include provisions by which service providers *may* be compensated, it remains to be seen whether the full costs of what is involved will be covered going forward. If adequate reimbursement is less forthcoming in these tough economic times, it seems inevitable that service providers will have to pass the costs on to their customers, meaning that companies such as database marketers could also be affected.

REFERENCES AND NOTES

- 1 Data Retention Regulation (SI 2007/2199).
- 2 Nettleton, E. and Watts, M. (2007) Assessing the costs of data retention in the UK. *Journal of Database Marketing and Consumer Strategy Management* 15(1): 56–59.
- 3 Nettleton, E. and Watts, M. (2006) The data retention directive. *Journal of Database Marketing and Consumer Strategy Management* 14(1): 74–77.
- 4 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
- 5 Walker, C. (2009) Data retention in the UK: Pragmatic and proportionate, or a step too far? *Computer Law & Security Review* 25: 325–334.
- 6 The Data Retention (EC Directive) Regulations 2009, No. 859.
- 7 See the Home Office Consultation, 'Protecting the Public in a Changing Communications Environment', April 2009 and the summary of responses to the consultation both of which are available from the Home Office website at <http://www.homeoffice.gov.uk/documents/cons-2009-communication-data/>.
- 8 See Article 11 of the 2009 Regulations.

- 9 Though not covered here, it should be noted that a separate consultation was also launched by the Government on 17 April 2009 dealing with the issue of which public authorities should be entitled to obtain communications data under the Regulation of Investigatory Powers Act (RIPA) and for what purposes this should be allowed.
- 10 The latter proposals are currently subject to a separate consultation concerning the 'Knowing or reckless misuse of personal data – introducing custodial sentences' which opened on 15 October 2009 and can be found at <http://www.justice.gov.uk/consultations/misuse-personal-data.htm>.
- 11 See the Information Commissioner's Response at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_response_home_office_consultation_20090715.pdf.
- 12 House of Lords Hansard, Tuesday 22 July 2008 (though seemingly the figures were not included in the Hansard entry for the question put by The Earl of Northesk).
- 13 For more details see the Register article 'UK.gov dishes out £19m for comms snoop data silos' posted on 6 August 2008 which is available at http://www.theregister.co.uk/2008/08/06/data_retention_grant_spending/.