Caution required in the evolving data retention environment

Will the new government attempt to resuscitate its predecessor's plans to impose greater obligations on telecommunications providers to retain and analyse communications data? **Mark Young** urges them to tread carefully.

In light of the previous government's travails in Strasbourg over the DNA database[1] and the ongoing EU Commission investigation into the UK legal regime on confidentiality of communications and intercepts,[2] this brief comment urges UK policymakers to exercise caution in this area, and considers potential changes to the data retention framework in the broader EU context.

The Interception Modernisation Programme

The Home Office set out proposals last April[3] to extend requirements on Communication Service Providers (CSPs) to collect, retain and use communications data (essentially data about who contacted whom, when, for how long and from what location):

- CSPs would be required to collect and retain even more communications data than they do at present, including data that they do not process for business purposes, such as data relating to Internet-based services and communications services provided from outside of the United Kingdom, as well as communications data that they are not required to retain under the Data Retention (EC Directive) Regulations 2009;[4]
- CSPs also would be required to organise and process these additional communications data, matching third party data to their own data where they have features in common (for example, where it relates to the same person or to the same communications device).

The previous government's stated objective for this initiative, known as the Interception Modernisation Programme (IMP), was to keep up with developments in communications technology and "to find ways both (i) to ensure that all the potentially relevant data is collected and retained; and (ii) that it is done in a way that allows public authorities to put together an increasing number of fragments to make a coherent whole".[5] The government framed the IMP as an attempt to "maintain" the existing capability of public authorities to access and use communications.

Several respondents to the consultation took issue with this characterisation. Many criticised the proposals for blurring the currently distinct legal regimes for authorising access to communications data and intercepting content, and, aside from the not inconsequential matter of costs, queried whether CSPs would be able to implement such elaborate collection and retention systems.[6] The Information Commissioner's Office (ICO) certainly did not accept that the IMP was merely about preserving the status quo; on the contrary, it expressed in stark terms that the proposals would "represent a step change in the relationship between the citizen and the state".[7]

Although the IMP was reported to have been shelved last autumn, it is likely to be re-appraised by the Home Office and to return in one guise or another. Should this occur, to avoid further embarrassment in Strasbourg or wrangling with the EU Commission, the new government may be well advised to pay more than mere lip service to the principles of necessity, proportionality, oversight and accountability – principles that derive from established European human rights law and which the Home Office claimed to uphold, but which extensive and vague data retention plans such as the IMP potentially violate.

IMP and European Human Rights Law

Access to communications data and use of surveillance powers by over-enthusiastic officialdom has understandably piqued the interest of the press in recent years.[8] Although access to data is an important issue, there is a danger that it obfuscates the more fundamental question about whether the initial collection and retention of data is lawful (as distinct from secondary considerations about how such data are accessed or used).

The European Convention on Human Rights specifies that public authorities may only interfere with the right to respect for private and family life in narrowly-defined circumstances (Article 8(2)). In particular, any interference must be in accordance with the law and necessary in a democratic society, in view of such public interests as national security, public safety and the prevention of disorder or crime.

The European Court of Human Rights (ECHR) has established in a series of decisions that the mere retention of data relating to the private life of an individual, such as communications data,[9] constitutes an interference with an individual's right to privacy under Article 8[10] – regardless of whether public authorities make any subsequent use of that data.[11] Article 8 helps protect the right to personal development and to establish and develop relationships with other human beings and the outside world.[12] Wide-ranging retention plans such as IMP may dissuade people from using certain technologies and thereby interfere with these important aspects of the right to privacy under Article 8.

When it published the IMP proposals last April, the Home Office claimed that the legal framework regarding retention and access to communication data was based upon the principles of necessity and proportionality. But under Article 8(2) an interference will only be considered "necessary in a democratic society" if it is for a

pressing social need and is proportionate to the legitimate aim pursued[13] – standards that such vague proposals arguably fail to meet.

Although the government set out why communications data can serve an important purpose in the fight against crime, it did not explain what pressing social need would justify the collection and retention of every single piece of communications data that CSPs could process. And because CSPs would be required to collect, retain and process vast quantities of information – far in excess of the amount of information law enforcement agencies may actually need – the proposals seemed to be disproportionate to the government's claimed legitimate aim to fulfil its duty to protect the public. The Home Office even seemed to admit as such when it stated that "public authorities will only ever access a very small proportion of the data that communications service providers will continue to collect and retain".[14] This statement presumably was intended to allay fears regarding who may access the data, but seems only to betray a failure to analyse the legality of retaining and processing additional data in the first place.[15]

Case law of the ECHR has also established that proportionate safeguards must be put in place to ensure that any interference is no greater than necessary,[16] especially in cases involving the automatic processing of personal data and when such data are used for police purposes.[17] Measures are unlikely to be regarded as necessary if there are alternative and less invasive methods of achieving the legitimate aim in question.[18] Unfortunately, the Home Office neither provided details about how additional communications data would be retained nor established restrictions regarding how commercial entities charged with retaining the data may use them. In response, the Information Commissioner (and others) pointed out that there may be less invasive alternatives to pursue the government's aims, including targeting specific phone numbers, only permitting the collection of communications data in relation to specified suspect individuals (and possibly their associates), or restricting such interference to instances where there is a significant risk. [20]

Finally, to be deemed to be "in accordance with law" and justify an interference with private life under Article 8, measures must be adequately accessible and precise[21] to enable an individual to regulate his or her conduct in order to avoid the interference.[22] But because blanket proposals such as IMP could be deemed excessively arbitrary[23] and to lack sufficient clarity,[24] there is a significant risk they also could fail to meet these requirements.

It seems likely that vague and extensive retention measures similar to the IMP would struggle to meet all of the requirements that permit an interference with private life under Article 8. The UK is already under European Union scrutiny in relation to its legal regime on confidentiality of communications and intercepts. The Commission is currently considering the Home Office's January response to the Commission's second phase of infringement proceedings, and whether to refer the case to the European Court of Justice – and could well avoid further confrontation regarding these related issues.

The broader picture for data retention

Even without enhancing requirements, European data retention laws continue to cause controversy, for example in Germany, Ireland and Romania. Questions about the constitutionality of European data retention laws emphasise the difficult relationship between data retention and data protection regimes, and underline the timeliness of the EU Commission's current review of the Data Protection Framework and evaluation of the Data Retention Directive.

The Commission has been evaluating the implementation of the Data Retention Directive across Member States, and will adopt an evaluation report in autumn 2010. A legislative proposal to amend the Directive may follow. The Commission's evaluation report is likely to focus on the inconsistent applications and interpretations of the Directive that cause significant problems in practice. For example, there is a lack of clarity over which service providers are obligated to retain data, as well as regarding the categories of data that they must retain. Although the Directive applies only to electronic communications services ("ECSs"), there is disagreement across and even within Member States as to what services constitute ECSs. Member States also require that different types of data should be retained. These issues are made more complex because there is no harmonised period for the retention of data – some Member States apply a six month retention period, while others have opted for 12, 18 or 24 months – nor clear rules governing access to or jurisdiction over data. Further, although the purpose of the Directive is to ensure that data are available for investigating, detecting and prosecuting serious crime, national definitions of "serious crimes" vary to a significant degree.

Problems with the data retention framework are magnified by the transition to cloud computing models. First, there is a danger that providers of "information society services" may incorrectly be deemed to be ECSs and therefore subject to the Data Retention Directive (a provider may even be considered an "information society service" in one country and an ECS in another). In the rare instances where a cloud provider offers services that qualify it as an ECS, existing legal divergences are likely to create difficulties, as cloud operations necessarily span several jurisdictions; for example, a provider's compliance with a six-month retention mandate of one country may violate a two-year mandate arising in another. This makes it impossible for providers to have a single, coherent and cost-effective internal retention policy and set of procedures, which results in confusion among users, undermining their confidence in and willingness to use new technologies and services. Industry is understandably concerned that this lack of consistency and harmonisation regarding data retention rules could create obstacles to the deployment and uptake of cloud services in Europe – a key aim of the new Commission under the new Digital Agenda portfolio. Over the next 18 months, the Commission will have to set out how it intends to address these challenges.

Conclusion

Returning to the UK, the Conservatives

vowed last September to submit any Home Office proposal for the retention of (and access to) communications data to the UK Information Commissioner for pre-legislative scrutiny, and that all future proposals regarding data collection and sharing would be subject to privacy impact assessments.[25] Adopting such precautionary measures is likely to be welcomed by industry and civil liberties campaigners alike. It also might help avoid further scathing judgments from the ECHR or investigations by the European Commission, which, given the elevated status of protection for personal data following the Lisbon Treaty and initiatives under the Stockholm Programme, is likely to play an ever-increasing role in determining future data retention laws and policy in the UK and beyond.

AUTHOR

Mark Young is Associate in the European Data Privacy Group, Covington & Burling LLP
Email: MYoung@cov.com

REFERENCES

1. *See* the strongly worded judgment handed down by the European Court of Human Rights in *S & Marper v UK* (Apps. 30562/04 and 30566/04), 4 December 2008, http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=marper&sessionid=52728462&skin=hudoc-en
2. This complaint was initiated in relation to the use of deep packet inspection technology and the UK's alleged failure to comply with EU rules protecting the confidentiality of electronic communications, see IP/09/1626, Brussels, 29 October 2009, *Commission steps up UK legal action over privacy and personal data protection*, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1626
3. Home Office Consultation, *Protecting the Public in a Changing Communications Environment*, www.homeoffice.gov.uk/documents/cons-2009-communication-data/
4. These regulations, which implement the DRD with regard to the retention of communications data relating to Internet access, Internet telephony and Internet email, only came into force in April 2009. Understandably, the UK Information Commissioner queried, in response to the proposals, whether the government had given the new arrangements enough time to work, see ICO response to the Consultation Paper, 15 July 2009, para. 4.7, www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_response_home_office_consultation_20090715.pdf
5. Home Office Consultation, supra note 5 at p. 22.
6. See*, for example*, LSE Briefing on the Interception Modernisation Programme, www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf
7. See ICO response to the Consultation Paper, supra note 6 at 1.6.
8. *See, for example*, *Telegraph*, 11 April 2008, *Poole council spies on family over school claim*, www.telegraph.co.uk/news/uknews/1584713/Poole-council-spies-on-family-over-school-claim.html
9. Data retention is no less an interference in private life when it is limited to communications data, as opposed to the content of communications, see *PG and JH* v. UK (App. 44787/98), 25 September 2001, 2001-IX. *See*, also, the ICO statement on the Communications Data Bill, 27 April 2009, www.ico.gov.uk/upload/documents/pressreleases/2009/ico_statement_dc_bill.pdf
10. *Leander v. Sweden* (App. 9248/81), 26 March 1987, A 116 (1987), 9 EHRR 433.
11. *Amann v. Switzerland* (App. 27798/95), 16 February 2000, 2000-II, 30 EHRR 843.
12. *Burghartz v. Switzerland* (App. 16213/90), 22 February 1994, A 280-B (1994), 18 EHRR 101, opinion of the Commission, p.37, para. 47; *Friedl v. Austria* (App. 15225/89), 31 January 1995, A 350-B (1995), 21 EHRR 83, opinion of the Commission, p.20, para. 45.
13. *Foxley v. UK* (App. 33274/96), 20 June 2000, 31 EHRR 25; *Handyside v. UK* (App. 5493/72), 25 June 1997, A 24 (1976), 1 EHRR 737; *Olsson v. Sweden (No 1)* (App. 10465/83), 24 March 1988, A 130 (1988), 11 EHRR 259; *Klass v. FRG* (App. 5029/71), 6 September 1978.
14. Home Office Consultation, *supra* note 5 at p. 28; further, the Government acknowledges at p. 13, "The vast majority of all communications data that is collected and retained today is never accessed by public authorities".
15. Some may find this particularly surprising given that the ECHR unanimously ruled in the high-profile decision of *S and Marper v United Kingdom* — a mere four months before the IMP consultation paper — that the UK government's policy of systematically and indefinitely retaining DNA material of any person of any age suspected of any recordable offence was disproportionate.
16. *Foxley v. UK, supra* note 15.
17. *S and Marper v. UK, supra* note 3, para. 103. The case repeated that in circumstances where communications data undergoes automatic processing, as envisaged under the IMP, there must be legislation in place which is proportionate and not excessive in relation to the purpose and duration of storage.
18. *Peck v. UK* (App. 44647/98), 28 January 2003, 2003-I, 36 EHRR 719.
19. *See* ICO response to the Consultation Paper, supra note 6 at para. 1.2.
20. *Id.* para. 4.4.
21. The ECHR has interpreted "in accordance with law" to mean that not only must a law authorising the interference be in place, but it should meet the standards of accountability and foreseeability inherent in the rule of law, see, *Malone v. UK* (App. 8691/79), 2 August 1984, A 82 (1984), 7 EHRR 14.
22. *Liberty and others v. UK* (App. 58243/00), 1 July 2008, 48 EHRR 1.
23. The requirement of foreseeability is not satisfied by blanket measures that allow everyone to foresee that the state will interfere with their right to a private life (*Malone v. UK*, *supra* note 23, para. 67). Indeed, what makes a law foreseeable is the extent to which it distinguishes between different classes of people, thereby placing a limit on arbitrary enforcement by the authorities (*see, for example, Kruslin v. France* (App. 11801/850) 24 April 1990, A 176-A (1990), 12 EHRR 547; *Amann v. Switzerland, supra* note 13).
24. The ECHR has indicated that legislation should be precise and clear (especially as technology becomes more sophisticated) and specify, for example, the limits on how long data may be retained and the categories of people against whom surveillance measures may be taken, *see Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (App. 62540/00), 28 June 2007; *Weber and Saravia v. Germany* (App. 54934/00), 29 June 2006; *Prado Bugallo v. Spain* (App. 58496/00), 18 February 2003; *Lavents v. Latvia* (App. 58412/00), 28 November 2002; *Niedbala v. Poland* (App. 27915/95), 4 July 2000.
25. "Reversing the rise of the surveillance state", 16 September 2009, www.conservatives.com/News/News_stories/2009/09/Reversing_the_rise_of_the_surveillance_state.aspx