



## Joint Committee on the draft Communications Data Bill

### Submission by the Law Society of England and Wales

*The Law Society of England and Wales ("The Society") is the professional body for the solicitors' profession in England and Wales, representing over 150,000 registered legal practitioners. The Society represents the profession to parliament, government and the regulatory bodies and has a public interest in the reform of the law.*

- I. Historically English law has protected privacy in particular circumstances but has never accepted a general right to privacy. The Human Rights Act 1998, by incorporating the European Convention on Human Rights (ECHR) into English law, changed that. Via the incorporation of Article 8 of the ECHR, English law now recognises a qualified right to respect for private and family life. This general right is supplemented by the data protection framework enshrined in the EU Data Protection Directive and the UK's Data Protection Act 1998.
- II. Effective data privacy and data protection rights are essential to life in an Information Society. The vast quantities of personal data generated by digital technologies of all kinds mean that without constant vigilance, and some restraint by the State, personal data privacy will quickly collapse. It is worrying, therefore, that the Government's plans will compel organisations to collect information about their users that they would not have previously had a reason to capture, using technology mandated by and for the purposes of the Home Office.
- III. It is essential to recognise that, rightly or wrongly, the Government's proposals are highly intrusive. The Government has emphasised that its proposals involve the retention of, and access to, communications data not content. The implication is that they are only mildly intrusive. However, as the Information Commissioner points out: 'You can tell an awful lot about some people's personal circumstances from the people they are talking to and the websites they visit'.<sup>1</sup> Indeed, it would scarcely be worthwhile from the Government's perspective to introduce this measure if you could not.
- IV. The Government has also sought to distinguish its proposals from those of the Communications Data Bill 2008 by emphasising that there are no plans to create a single government database. These earlier proposals were scrapped, in light of widespread condemnation from politicians of all parties, as well as non-politicians. It is clear that a single, central database captures the public imagination in a way that highlights the privacy and security issues at stake; it is not clear, however, that numerous privately owned databases are less privacy intrusive. Mass surveillance of innocent people is still being proposed.
- V. A comprehensive review of the legal, institutional and technical framework within which surveillance powers are exercised in the UK is long overdue and, in this regard, the Protection of Freedoms Act 2012 (POFA) was a missed opportunity. In particular, the Law Society has repeatedly called for an overhaul of the Regulation of Investigatory Powers Act to ensure explicit protection of communications between lawyers and their clients, which is a common position across the legal profession.

---

<sup>1</sup> Information Commissioner's statement on the Communications Data Bill, 27 April 2009

- VI. The Society welcomes the Joint Committee's pre-legislative scrutiny of the draft Communications Data Bill and the challenging questions on which it has invited comments and on which the Society offers its views below.
- 

**1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?**

- 1.1. The broad objectives of the Bill are clear. That is, to ensure that communications data from internet-based communications (instant messaging, social networks etc) are obtained and retained by CSPs and can then be obtained by authorised public authorities in appropriate circumstances.

**2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?**

- 2.1. The Government's case is that communications data have played a role in all major Security Service counter-terrorism operations and most serious organised crime investigations. It now argues that lack of communications data is beginning to hamper investigations.
- 2.2. The Law Society's view of this argument mirrors that of the European Data Protection Supervisor (EDPS), Peter Hustinx, in relation to the European Data Retention Directive. Hustinx has argued that if a measure is already in place and practical experience has been gained 'there should be sufficient qualitative and quantitative information available which allows an assessment of whether the measure is actually working and whether comparable results could have been achieved without the instrument or with alternative, less-privacy intrusive means. Such information should constitute genuine proof and show the relationship between *use* and *result*.<sup>2</sup> Hustinx concluded that the quantitative and qualitative information provided by Member States was insufficient to confirm the necessity of data retention as required by the Data Retention Directive. In the Society's view the Government's published evidence-base for additional data retention powers is similarly weak.

**3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?**

- 3.1. The proposals in the Bill reinforce and extend an enabling framework in the UK that underpins what many, including the Information Commissioner, have called a surveillance society. The drift into a surveillance society is why the Society argues that POFA was a missed opportunity. The Society does, however, welcome the recognition in POFA of the principle of judicial approval for certain applications to obtain or disclose communications data. The case for extending this principle should form part of any future review of surveillance.

**4. What lessons can be learnt from the approach of other countries to the collection of communications data?**

- 4.1. The Law Society has not explored this question in any depth. However, the Society notes that Privacy International have claimed that the only other

---

<sup>2</sup> Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC). 31 May 2011

countries in the world that have the kind of mass surveillance systems that are proposed are China, Iran and Kazakhstan<sup>3</sup>.

**5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?**

5.1. The Society is not aware of any. The Society does think the Home Office should identify alternatives, publish the evidence for and against, and consult both experts and members of the public to ensure that we can have an informed debate.

**6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?**

6.1. The relationship between the Data Retention (EC Directive) Regulations 2009 and the proposals in the Bill is not entirely clear. The Regulations apply to communications data to the extent that such data are generated or processed in the UK by a telecommunications operator in the process of supplying a particular communications service. The draft Bill enables the Secretary of State to make an order to ensure that communications data are available to be obtained from telecommunications operators. The implication is that the data to be obtained under the Bill are not data that would be retained by operators in the normal course of their business. However, as the Home Office acknowledges, and the rationale for the Bill, is that the UK's telecommunications infrastructure is changing rapidly. It follows that the boundary between data that will be retained in the course of business and data that will not is also shifting (and not necessarily simply in the direction of less data retention for business purposes) On the face of it, therefore, one overarching piece of legislation would be preferable.

**7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?**

7.1. Civil liberties should not be traded in this way. If the provisions of the Bill are wrong they should not be adopted; if other measures deserve to be scrapped on human rights grounds they should be.

**8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?**

8.1. This is a question for CSPs.

**Costs:**

**9. Is the estimated cost of £1.8bn over 10 years realistic?**

9.1. The Society does not take a view on this matter.

**10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?**

---

<sup>3</sup> Privacy International, *Submission to the Joint Committee on the draft Communications Data Bill*

10.1. No comment.

**Scope:**

**11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?**

11.1. No comment.

**12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?**

12.1. The limited evidence provided by the Home Office explaining the need for this Bill concerns Security Service anti-terrorist operations and serious and organised crime investigations. Limiting access to the Security and Intelligence Services (for their statutory purposes) and to the police for the investigation and detection of serious crime would be appropriate.

12.2. It should not be possible for the Secretary of State to vary the list by Order. Parliamentary debate and approval should be necessary before any extension of access is permitted.

**13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?**

13.1. It seems entirely unrealistic to pursue overseas providers. The Home Office should explain how its plans will work in practice.

**Use of Communications Data:**

**14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?**

14.1. As stated above (Q.12), in the absence of any clearer justification, limiting access to the Security and Intelligence Services (for their statutory purposes) and to the police for the investigation and detection of serious crime would be appropriate

**15. Is the proposed 12 month period for the retention of data too long or too short?**

15.1. Without a stronger evidence base it is unclear whether or not any retention is necessary and, if it is, whether 12 months is too long or too short. The Home Office should explain the basis on which 12 months has been chosen.

**Safeguards:**

**16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?**

16.1. As the Society explained in its introductory statement, the Society regards these proposals as highly intrusive and does have concerns about compliance with Article 8. Independent judicial review would be better. In cases of urgency such review might need to take place *after* communications data had been accessed. Such cases should be exceptional.

**17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?**

17.1. A warrant system would be appropriate. It should apply to all public authorities. Any evaluation of the resource implications should take into account the probable reduction in the number of applications for communications data.

**18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?**

18.1. Yes, if the Offices which support them are properly resourced. Oversight arrangements can only be effective if they can be implemented in practice and the Information Commissioner has already highlighted the need for additional resources.