Evidence submitted to the Joint Committee on the draft Communications Data Bill

Zoe O'Connell - 23rd August 2012 - zoe@complicity.co.uk

Qualifications

1. I have worked in the service provider industry continuously since graduating from Brunel University with a degree in Computer Science in 2000 and have maintained an interest in digital policy since that time, starting with the passage of the Regulation of Investigatory Powers Act. I am also qualified as Cisco Certified Internetwork Expert (#8174), a top-level qualification in the networking industry.
2. I currently work for a medium-sized AIM-listed managed service provider in South East England, where my role as the senior networking professional includes dealing with requests under the existing Regulation of Powers Act. In that capacity, I was also involved as a witness in what I believe to be the first conviction for "inciting terrorist murder via the internet". (R v Tsouli, Mughal & Al-Daour, 2007)
3. I am also author of the blog "Complicity". All answers in this submission are my personal opinion.

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

4. Considering the draft bill itself, there is no apparent restriction on the powers that are granted by it, which does not give any way of assessing exactly what the intentions are. The powers could be used for deployment of "black boxes" en mass throughout the UK, could be used to just to target known hotspots, or could just be used to attempt to intercept information to and from non-cooperative web site owners. They may even be no deployment of interception, with the bill just being used to retain. additional information.
5. In it's publicity surrounding the bill, the Home Office (HO) stated legislation was needed because "*New communications technologies are generating communications data in different ways and communications data is* ***no longer always retained*** *by communications service providers."* (Emphasis added) In oral evidence to the committee, Charles Farr and Richard Alcock also concentrated on the "data retention" aspect of the bill as being primary, rather than obtaining data via interception. (This is discussed further in answer to question 2)
6. It would therefore seem that the HO are publicly trying to state that the bill is about retention. However, the powers being asked for include obtaining data via interception, and the use of these powers has not been made clear or publicly discussed in any detail by the HO.
7. The Home Office (HO) has also stated that it has spoken to a number of service providers who do understand their aims here. However, it is certainly not clear to myself or to anyone else I have spoken to in the industry what the aims are. It may be that those who have been spoken to are not themselves technical, but instead managers in effect bidding for a slice of the £1.8bn on offer. As a result, without knowing who the HO have been communicating with, one should be wary of accepting assurance that the concerned service providers are happy (technically or otherwise) with the HO proposals. Even if the HO genuinely believes the

assurances given to it by service providers, the assurances it has received may not be entirely have been made in good faith and from a disinterested position.

8. Multiple Freedom of Information requests have been made to the Home Office on the topic of who they have spoken to, both for the draft bill and existing data retention regimes, and also enquiring as how they arrived at the costs stated. All have been entirely or mostly refused[1], so there is no clarification available via that route as to either the value of any assurances apparently given by service providers or the aspirations of the bill in general.

9. Other potentially useful information on the bill has also been suppressed by the HO. For example, they attended a conference run by the London Internet Exchange (LINX) and presented a half hour slot to Internet Service Providers (ISPs) on the bill. The conference attendees were not security cleared and include foreign nationals, but despite this the HO refused permission to allow LINX to release the video for download to members who were not present at the meeting and additionally stated that they would never disclose who in the industry they had talked top in order to stop people simply switching ISPs.

10. The above facts combined - overly broad content in the bill, concentration on "data retention" in evidence to the committee, refusal to answer Freedom of Information requests and limiting circulation of information would suggest that the HO simply does not want more than vague details of it's aims to be public knowledge for security reasons. That approach makes any useful, democratic assessment of their request a practical impossibility and also seriously damages any prospect of meaningful oversight.

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

11. In evidence given orally to the committee by Charles Farr, Director General of the Office for Security and Counter-Terrorism, states that much of the current problem is down to "ambiguity" in the Data Retention Directive (Q7) and also goes on (Q9) to state that he believes the draft bill will increase the proportion of successful requests for data from 75% to 85%. This concentration on data retention (Versus data acquisition) is further reiterated, including in a response to Question 74 by Richard Alcock (Director of Communications Capability Directorate) in his answer to Q74, who states that the costs are around data retention.

12. What is not addressed is why simply updating the UK implementation of the data retention directive would not be sufficient to achieve the stated 10% uplift if this is simply a data retention issue.

13. There is mention in the same session of cooperating with European, not UK, providers in retaining this data and that differences in the implementation of the Data Retention Directive (DRD) across Europe were part of the problem. It is not explained how a bill passed in the United Kingdom could be used to require

1 http://www.whatdotheyknow.com/request/external_organisations_consulted, http://www.whatdotheyknow.com/request/data_retention_ec_directive_regu_3, http://www.whatdotheyknow.com/request/reimbursements_to_csps_for_data, http://www.whatdotheyknow.com/request/payments_under_regulation_of_inv, http://www.whatdotheyknow.com/request/internet_monitoring_systems

European providers to retain data: Either the providers somehow fall under UK law by virtue of doing business here (In which case they would be subject to a UK "clarification" or update of the Data Retention Regulations 2009) or they are not subject to UK law, in which case any agreement with them would not be influenced by new legislation.

14. Although effort has been made to justify retention of additional data, no serious attempt appears to have been made by the Home Office for additional powers of interception and obtaining additional data.

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

And:

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

15. Based on an analysis of data released by Google[2], the UK has per capita the population most investigated via data communications in the world. Other countries may engage in snooping directly on their citizens, rather than requesting data from countries such as Google, but the UK would be unique amongst western democracies should it engage in such practices and this would largely be uncharted territory.

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

16. As discussed previously, updating the Data Retention (EC Directive) Regulations 2009 to cover more data should be considered. However, the HO have been reluctant to release enough information on what they hope to achieve which makes proper consideration of any alternatives difficult.

QUESTION 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?

17. It would appear that, as written, the bill would supersede the Data Retention Regulations in all respects. There would appear to be no circumstances under which it would be worthwhile for the Secretary of State to issue further notices to service providers under section 10 of the regulations should the bill be passed. As a result, the regulations would cease to have any real world effect once all current providers are notified of their new obligations under the proposed bill.

QUESTION 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?

18. The draft bill gives the potential for near-total omniscience to the state within the communications world. Given that people's lives are increasingly integrated with electronic devices and the Internet, the scale of any scrapping of existing powers

2 http://www.complicity.co.uk/blog/2012/06/google-data-shows-uk-back-as-most-snooped-on-population/

outside of the bill itself to rebalance liberties would have to be staggering in it's scope.

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

19. Despite multiple Freedom of Information requests, as noted in the answer to Question 1, the HO has yet to produce any breakdown of it's costs beyond simply stating around half the cost is retention. As it has also not been made clear what the aims and objectives of the bill is, it is not possible to determine if this is realistic.

QUESTION 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?

20. The HO have not released any breakdown of this benefit, so it is hard to analyse. It would appear some of these benefits, based on evidence given orally by Charles Farr, is based on notional values of human life etc, for which we do not have numbers.

21. However, a basic sanity check can be performed. There were 414,400 successful requests in 2010 (75% of 552,550) and the HO have stated in oral evidence to the committee that they hope for a 10% increase in successful requests as a result of the bill, meaning an additional 55,255 requests. This would mean that the current Data Retention regime is delivering a value of £3.75bn per year, or £9k per request. That number seems large and I would have expected to see more publicity surrounding the benefits of the existing system, but is a feasible figure given that the HO aims to *"prevent revenue loss through tax fraud and facilitating the seizure of criminal assets".*

QUESTION 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?

22. The UK would appear to have no legal recourse against foreign service providers who do not, entirely voluntarily, comply with the proposed bill. If the HO did attempt to find a way to pursue foreign service providers with no UK base, this would set a very unwelcome precedent. UK service providers may then have the burden of complying with laws and regulations in every other country connected to the Internet, in case a user from that country visits their site.

QUESTION 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?

And

QUESTION 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?

23. Independent oversight of requests is certainly desirable, but a "warrant" could be granted by the Secretary of State or their nominated representative, which lacks sufficient independence. It would be more appropriate to specify that a judicial warrant is required.

24. The main objection to requiring warrants by the HO has been time, in critical cases, and cost. On the topic of time, there is no reason why the vast majority of non-time-critical (Priority Grade 3, under the current RIPA system) should not require warrants. Such a system must mandate retrospective judicial approval of any high priority (Grade 1) requests to prevent abuse, with automatic reporting of any failed retrospective requests and investigation by the commissioner. The commissioner has already identified "serious non-compliance" by a number police forces under the current oral approval system[3] which is a major cause for concern if not addressed.

25. For cost, the overall cost of the proposed system amounts to £3,257 per successful request[4]. The cost of applying for a warrant does not appear to constitute a major additional burden in light of this.

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

26. The roles in theory are welcome, but the commissioners have proven themselves to be relatively toothless and do not properly investigate problems. A much stronger system of oversight is required.

QUESTION 19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

27. As noted previously the HO have been extremely reluctant to provide any information to the committee in evidence to support the bill. There is no reason at this stage to believe they would be any more cooperative when it comes to future oversight. The draft bill should enforce tough, thorough and public reporting by the HO and all organisations granted powers or obligations under the bill.

28. It is notable that the proposed system of interception involves the secretary of state mandating the equipment and configuration to be used by service providers, meaning it is unlikely that service providers will have any meaningful insight into the operation of the system. This will mean that the only organisations who really know what is going on are the HO and the (So far unidentified) suppliers of the equipment. This potentially means that no independent oversight of the technical implementation of the bill will exist at any level.

QUESTION 21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

29. It should be a criminal offence to wilfully disregard any communications data provisions, to prevent managers and staff refusing to take responsibility for the significant powers granted to them, in a similar way to the driver of a vehicle - and

3 2011 Annual Report of the Interception of Communications Commissioner, Page 35
4 http://www.complicity.co.uk/blog/2012/07/comparative-costs-of-ccdp-requests/

not his employer - being liable for offences committed behind the wheel. However, history has shown that prosecutions for such offences rarely take place as they are deemed not to in the public interest and this is as critical a problem as the penalties themselves. Mandating investigation by the commissioner with a strong presumption of prosecution on behalf of the CPS would go some way to solving this issue.

QUESTION 22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

30. On the scale required by the HO, no. No evidence has been presented by the HO to suggest otherwise, or how they would handle non-standard and ever-evolving protocols used by many sites.

31. As an example, in the 2010 film "Four Lions", the jihadists converse over a web site that appears to be based on Disney's "Club Penguin", an online game for children. The protocol used for communication between such sites and the client software running on the users computer will be completely proprietary and change entirely at the whim of the developers.

QUESTION 23. How safely can communications data be stored?

32. Security is a trade-off between usability and accessibility of the data versus it's value and the impact if it is compromised. The value of the data held by Service Providers will be huge, representing a valuable asset in corporate espionage potentially funded by foreign governments.

33. Such a high-value asset needs to be protected very robustly and although service providers generally have a good track record in keeping critical data secure, breaches do happen. This is a significant risk, the impact of which should be properly and fully investigated and reported on by the HO and accepted as being necessary prior to the bill being passed.

QUESTION 25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?

34. It would seem to be trivial to circumvent, unless the HO has some mechanism of decrypting all traffic that is not known to the rest of the world. (See discussion in answer to Q26 for more on this)

35. The government of China, which has thrown significant resources at it's "Great Firewall of China" project, has been trying to simply block - not even intercept - unapproved internet sites. Despite this, it remains the case today that people are able to bypass this system using technologies such as "tor". There is no reason to believe the HO would be significantly more successful at interception than other governments would be at the simpler task of blocking.

QUESTION 26. Are there concerns about the consequences of decryption?

36. Potentially, yes, as we do not know how the HO intends to break decryption other than a simple statement that they can. There is a real danger that "man-in-the-middle" attacks on encryption might expose UK users to additional security risks or

generally destabilise the internet in unwelcome ways[5]. To avoid security and stability problems created by interception, it should be a requirement of the bill that interception may only be passive and not alter the contents of the communication in transit.

37. Worse, in a nightmare scenario, whatever technology is deployed at the service provider level by the HO to decrypt traffic is stolen from a data centre by criminals or members of foreign intelligence agencies, potentially exposing very large number of users to security risks and huge financial implications.

5 http://www.complicity.co.uk/blog/2012/06/spooks-in-the-middle/