2012 - Joint Committee on the draft Communications Data Bill

This is the submission of the JNT Association, trading as Janet, to the Joint Committee on the draft Communications Data Bill [1]. Janet is the UK's National Research and Education Network, a high-speed private data network that connects all universities, colleges, research organisations and schools networks to each other and to the public Internet.

We are concerned that the draft Bill will, perhaps unintentionally, affect a much wider range of networks, data and users in the UK than the current Data Retention Regulations (Q1, 2, 11), and that it could damage the reliability of, and confidence in, computers and networks that is essential if the UK is to achieve the social and economic benefits of an information society (Q9, 26). We also believe that the possibility of many new processes for obtaining communications data will lead to confusion and create new opportunities for unauthorised access to that data (Q16, 23, 26).

Q1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

Q2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

The draft Bill would give the Secretary of State the power to order the collection of communications data from any "telecommunications operator"; this is defined in clause 28(1) of the draft Bill so as to include public and private networks both inside and outside every organisation in the UK as well as a high proportion of domestic properties. Current data retention requirements only apply to the much smaller number of public communications providers, as defined in Regulation 2(e) of the *Data Retention (EC Directive) Regulations 2009* , deriving from s.151 of the *Communications Act 2009*.

The Home Office's case for the Bill does not mention nor justify this significant increase in the networks, organisations and users that may be subject to data retention requirements, nor can we see any need for it to achieve the Bill's stated purpose. We therefore recommend that the scope of the Clause 1 power be reduced to "public communications providers" as under the current data retention regime.

Q9. Is the estimated cost of £1.8bn over 10 years realistic?

The financial costs largely depend on how, and how often, the powers created by the Bill are exercised, so cannot be estimated from the information that has been published.

However we note that the powers may also impose non-financial costs on telecommunications operators and their services. Many networks, including Janet, have been designed to ensure that a single failure does not cause loss of connectivity. A side effect of

this improved resilience through the provision of multiple paths is to make it harder to collect communications data as there is no longer any single point where all data can be collected. The Bill appears to give the Secretary of State the power to order such resilience to be removed to facilitate the availability of communications data, even though this would make the network unsuitable for the growing range of teaching, research and operational purposes that depend on highly-reliable networks. An order to add new monitoring devices into a network, or to alter the normal traffic routing, could also have an unpredictable effect on its reliability and performance.

The Bill may also require telecommunications providers to install and manage new systems to collect communications data, and will require them to keep collected data secure. This will require continuing effort by expert network and security engineers and privacy specialists. Organisations that have such specialists will forgo part of their contribution to the development and operation of products and services; organisations that do not currently have such skills will need to recruit them in areas subject to skills shortages.

Q11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

The draft Bill does not use the term “communications service provider”, which only appears in the Notes. The draft Bill instead defines and uses the term “telecommunications operator”. We do not consider that either the definition of “telecommunications operator” or “communications data” (in clause 28(1)-(5)) is appropriate.

As in our response to Q1 & 2 above, we do not believe that “telecommunications operator”, as defined in clause 28(1) of the Bill is the appropriate scope for the clause 1 power.

The definition of “communications data” in clauses 28(1) to 28(5) will extend much wider than the normal meaning of that term (and the stated intention of the draft Bill) when it is applied to organisations such as universities, webmail and social network services, all of which appear to be included in the current definition of “telecommunications operator”.

This is because “communications data” is defined in clause 28(1) as the aggregate of “use data”, “traffic data” and “subscriber data”. Clause 28(5) then defines “subscriber data” as “information (other than traffic data or use data) held or obtained by a person providing a telecommunications service about those to whom the service is provided by that person”. In other words “communications data” will comprise all information held by the service provider about the individuals who use the service. In the case of a university or social network this would cover much more than is normally considered subscriber or communications data: for example it would include a student’s academic record or a member of staff’s personnel file. Indeed since, unlike clause 28(4) defining use data, clause 28(5) does not exclude the content of communications, it appears that communications data would also include the content of all the user’s messages that were held by the telecommunications operator.

To remove this problem the draft Bill’s definition of “subscriber data” should be replaced by a definition that states what subscriber data **is**, rather than what it is not.

Q16. 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?

The current *Regulation of Investigatory Powers Act* Part 1 Chapter II (RIPA) regime establishes a single, well-defined, process for accessing communications data. This has allowed communications providers to develop their own processes for handling RIPA notices through a single point of contact, ensuring that all disclosures of communications data are prompt, lawful and efficient. To promote such efficiency, the Home Office Code of Practice [2] prohibits any use of other powers to obtain communications data.

Clause 9(2) of the draft Bill would reverse this approach by permitting "any conduct" to be used to request or order the disclosure of communications data. Communications providers would no longer be able to adopt standard processes, since they might receive valid requests or instructions through any process and in any form that any designated senior officer considers necessary and proportionate. This will inevitably slow down the process of access to communications data and increase its costs. As discussed in our response to Q 23 & 25 below, we believe it will also increase the opportunity for fraudulent access to stored information.

Clause 9(3) encourages alternatives to the standard RIPA process (which is described in clause 9(3)(d)), by giving examples of "asking any person" – apparently including within a communications provider – who may be able to obtain communications data to do so; Clause 9(4) would then authorise "obtaining or disclosure... or any other conduct" by such a person, even if it would otherwise be a criminal offence for example under s.55 of the *Data Protection Act 1998*. Indeed clause 9(2) appears to allow such a person to be required, rather than just asked, to obtain and disclose data, which would make the RIPA process redundant. The existing RIPA process was designed to promote the interests of law enforcement, communications providers and users. We do not consider that creating alternative processes under clause 9(2) will be satisfactory for any of those interests.

Q23. How safely can communications data be stored?

Q25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?

It is highly unlikely that communications data (or indeed any other data) can be stored completely safely: there are examples of information being obtained without authorisation from both police [3]and ISP [4]databases. Successful attacks can use both technical and human weaknesses, as discussed in the Information Commissioner's reports "What Price Privacy [5]" and "What Price Privacy Now [6]". We are especially concerned that allowing multiple processes for obtaining communications data under Clause 9(2) – particularly since these processes can be less formal than the current RIPA one – will make it much easier for "blaggers" to obtain communications data by fraudulent impersonation. Telecommunications providers and others with access to communications data will be required by that Clause to respond to new and varied forms of legitimate request and order, making it much easier for a blagger to explain why his request varies from those that have been seen before. Protecting against this risk will require scrupulous checks by the recipients of all requests under Clause

9(2), thus delaying lawful access to data and increasing the workload for both providers and the designated senior officers with whom they will have to verify every new process.

The data collection and storage systems envisaged by the Home Office will represent attractive targets for those who wish to obtain data about users. Even if only local communications data is stored this will be in larger quantities than at present. However the Home Office have also indicated that it will be possible to obtain data about communications using third party providers; this can only be done by examining the content of communications and extracting communications data from it. Such systems will be a particularly valuable target for attack, since access (either through a human or technological attack) to such a system could provide the ability to read all the communications content that passes through it, as is reported to have happened to Vodaphone-Panaphon's systems in Greece [7].

Q26. Are there concerns about the consequences of decryption?

Our concerns that data storage and collection systems will be an attractive target for unauthorised access would be increased if those systems were storing or accessing the plaintext of information or communications that are currently encrypted. As well as the harm resulting from the loss of information considered sufficiently sensitive to justify encryption, even a rumour of unauthorised access to a decrypting system could damage public and business confidence in the Internet as a safe way to communicate. The Government's plans for an e-society depend on citizens and businesses being willing to send and receive sensitive private information over the Internet, whether to e-government, e-health or e-business systems. If individuals do not believe that browser-encrypted communications are safe then it will be difficult to persuade them to use these systems.

Links
[1] http://www.parliament.uk/documents/joint-committees/communications-data/commsdataCfE.pdf
[2] http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition
[3] http://news.bbc.co.uk/1/hi/uk/7033935.stm
[4] http://www.theaustralian.com.au/australian-it/telecommunications/anonymous-hackers-dump-stolen-data-belonging-to-australian-firm-aapt/story-fn4iyzsr-1226437681976
[5] http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf
[6] http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico-wppnow-0602.pdf
[7] http://spectrum.ieee.org/telecom/security/the-athens-affair/