Adrian Kennard
Andrews & Arnold Ltd
FireBrick Ltd
Downmill Road
BRACKNELL
RG12 1QS

25th November 2015

Written evidence regarding Investigatory Powers Bill.

Andrews & Arnold Ltd are a small but technical Internet Service Provider (ISP), and FireBrick Ltd are a manufacturer of routers, firewalls, call servers, VPN servers, and related equipment. I personally have extensive experience in technical and operational aspects of running an ISP for over 18 years, having written the underlying operating code of our core routers and equipment. I have previous experience in mobile telephony and landline telephones and exchange equipment.

Key points:-

- There are a number of privacy issues which cause concern, especially web logs and interference
- I feel the bill needs to clarify and limit scope of data retention order to be in line with the expectations of the Home Office and so as to minimise misuse by future governments
- I feel that the current proposed 100% cost recovery needs to be on the face of the bill
- I feel retentions orders should not be required to be secret, though operators may choose not to disclose details
- I feel that the usefulness of Internet Connection Records is over stated and misunderstood, and will also have diminishing use over time, so should be considered not cost effective now.
- There needs to be clarification on DNS traffic being “content”
- There needs to be clarification on interaction with Data Protection Act

Ethical/Privacy issues

I am quite sure there are a number of issues which are better addressed by organisations such as Privacy International, Open Rights Group or similar. However there seem to me to be some clear issues with the bill as follows.

---

1 Web logs

The explanatory notes and discussions with the Home Office make it clear that there is an intention for retention notices to require, in some cases, the logging of the web site name visited by an operator’s customers.

Whilst telephone call data records do reveal some information about the subject it is clear that retention of details of every web site visited reveals much more about a person. It can be used to profile them and identify preferences, political views, sexual orientation, spending habits, and much more. It is also useful to criminals as it would easily confirm the bank used, and the time people leave the house, and so on.

This is plainly sensitive personal information, and it is clearly a huge invasion of privacy to collect and retain this information on innocent people.

It is also a valuable target for criminals and so a risk for operators to retain this data.

There have been arguments that this is not lmass surveillance" as nobody will look at the logs unless you are later part of some investigation. However, I am quite sure the same argument would not work if, for example, the law required a camera in every room in your house. The fact the logs may not be looked at does not mitigate the obvious invasion of privacy and mass surveillance by the very collection and retention of these logs.

As this level of logging is a new power over and above existing retention regimes, it deserves even more scrutiny. **I feel that this level of logging is unjustified and not proportionate or ethical and should be specifically excluded from the bill.**

---

2 Equipment Interference

Equipment Interference (or legalised hacking) is one of the most intrusive powers in the bill. It therefore seems unconscionable that "bulk equipment interference" orders are included in the bill. This could literally be placing a camera in people's homes via they PCs and phones without them knowing. Equipment Interference can also impede operation of devices, and make it easier for criminals to access devices. Surely such an intrusive power, if allowed at all, should only be targeted at the most serious of criminal suspects? **I feel that bulk equipment interference should be removed from the bill.**

It also seems that one of the means by which equipment interference can be carried out is by exploitation of a vulnerability in a computer system. Where such a vulnerability is known by the intelligence services they have a clear moral obligation to responsibly disclose that vulnerability to the manufacturer so that it can be rectified. **I feel that use of vulnerability in equipment should not be permitted, as allowing them encourages the intelligence services to keep vulnerabilities secret, thus exposing everyone to increased risk of criminal activity.**

Technical/compliance issues

Data Retention

I was pleased to have the opportunity to discuss data retention with the Home Office yesterday thanks to the Internet Service Providers Association. The discussions were interesting. The main concerns from the ISPA members present, mostly quite small ISPs, is that they could be subject to a retention notice, and that such notice could require "Deep Packet Inspection" which would have significant cost implications.

---

3 Scope of retained data

It seems clear from the Home Office that they are intending to only serve notices on those larger ISPs that are already subject to notices, and with which they have already had extensive discussions. They have indicated that they are not intending to target smaller ISPs, and even if they did, that ISPs would not be expected to log and retain data for which they simply do not have such a capability, and that they would not expect any collection of "third party data" or information from "over the top services". However, the bill, as worded, does not embody these intentions. **We would like so see specific caveats in part 4. Specifically:-**

- 71(9) should make clear that data is only that which "*is generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person)*". This wording is from the definition of an "internet connection record" in 47(6) so clearly part of the intended description.
- That is made clear by a definition that "process" in this context means that the operator considers the data and takes some decision on it (such as routing packets) and not simply that the data passes through the ISPs network.

- 71 should also contain a restriction that it must be “reasonably practicable for the operator to collect and retain the data”.

None of these changes should impact the intentions of the Home Office. It would still allow the key aspects of logging that seem to be the intention of the Home Office:-

- An email provider to log email addresses as these are processed and logged.
- A telephony provider to log call records.
- A mobile operator to log SMS messages.
- An operator that uses a “web proxy” to log web site names visited.
- An operator that uses Carrier Grade NAT (CGNAT) to log NAT sessions (connections).

It would, however, limit the scope of future governments to expand the retention beyond current intentions without a change to the legislation. The wording chosen also fits in with the cost implications of the bill as they relate to the activities which would significantly increase costs for the ISP such as Deep Packet Inspection (DPI).

4 Use of the term “Internet Connection Record”

The explanatory notes, and one of the clauses in the bill, make use of the term “Internet Connection Record”. We are concerned that this creates the impression that an “Internet Connection Record” is a real thing, like a “Call Data Record” in telephony.

An ICR does not exist - it is not a real thing in the Internet. At best it may be the collection of, or subset of, communications data that is retained by an operator subject to a retention order which has determined on a case by case basis what data the operator shall retain. It will not be the same for all operators and could be very different indeed.

We would like to see the term removed, or at least the vague and nondescript nature of the term made very clear in the bill and explanatory notes.

5 Gagging

77(2) prohibits an operator for revealing the existence or content of a retention order. Whilst I can understand operation reasons for not revealing targeted intercept warrants, a retention order does not relate to a suspect or a case, and so has no reason to be secret.

The Home Office were quick to confirm that this clause is at the request of the larger operators with which they have had discussions, and whom do not wish to reveal the existence of notices.

This makes no sense. If an operator wants to keep a notice secret they can simply do so. If an operator wants to discuss the notice with equipment vendors, technical working groups and forums with other ISPs or even their customers they are prohibited from doing so. Also, this clause only prohibits the operator disclosing the notice, and does not prohibit the Secretary of State, the Home Office, the Investigatory Powers Commissioner or anyone else who may know of the order from doing so, and so it does not even meet the requirement of the larger operators.

This clause simply needs removing.

6 Cost recovery

The Home Office also indicated that, as now, that operators would receive 100% cost recovery.

It is worth noting that this bill is not an attempt to regulate telecommunications operators because they are operating business models that are offensive to society or otherwise engaged in activity that needs controlling! This bill is specifically to force operators to provide a *service* to the authorities to help with criminal investigations of other parties, where the telecommunications operator is not themselves in any way complicit or liable. It is clear, therefore, that the operator should receive at least 100% cost recovery for providing this service - indeed, for most services provided a company would expect to be able to make a profit.

As this is the current intention it seems sensible that the face of the bill should state clearly that at least 100% cost recovery applies, and not the current wording which simply guarantees that it is not actually "nil". There can surely be no objection unless the Home Office are planning to stitch up operators in future.

We would like to see the bill specifically state that at least 100% cost recovery applies.

---

7 DNS logs

It is not clear if there would be any logging of DNS requests. I specifically asked the Home Office if, under traditional call logging, the content of a call to Directory Enquiries would be recorded and logged by the operator. It seems not, and this seems to make clear that the content of such a call is "content" and not "communications data". As DNS is the equivalent service to Directory Enquiries for Internet Access, I feel that the definitions should make clear that DNS lookups, or indeed any form database access lookup, is to be considered content and not communications data. The communications data in such cases being simply that a connection (request/reply) was made to a DNS server and who made it - not the content of what was looked up.

We would like to see clear wording to exclude the content of a DNS request ,or other database query, from "communications data", and clearly define it as "content".

---

8 Justification for "Internet connection records"

In the briefing with the Home Office the bill was explained, and we heard a story very similar to Theresa May's comments along the lines of:-

"*Consider the case of a teenage girl going missing. At present we can ask her mobile provider for call records before she went missing which could be invaluable to finding her. But for Internet access, all we get is that the Internet was accessed 300 times. What would be useful would be to know she accessed twitter just before she went missing in the same way as we could see she make a phone call*"

Now, I am sure this is a well practiced speech, used many times before. I am sure the response has been nodding of heads and agreement with how important "Internet connection records" are, obviously.

However, in yesterday's meeting I, and other ISPA members immediately pointed out the huge flaw in this argument. If the mobile provider was even able to tell that she had used twitter at all (which is not as easy as it sounds), it would show that the phone had been connected to twitter 24 hours a day, and probably Facebook as well. This is because the very nature of messaging and social media applications is that they stay connected so that they can quickly alert you to messages, calls, or amusing cat videos, without any delay.

It should be noted that it is quite valid for a "connection" of some sort to last a long time. The main protocol used (TCP) can happily have connections for hours, days, months or even years. Some protocols such as SCTP, and MOSH are designed to keep a single connection active indefinitely

even with changes to IP addresses at each end and changing the means of connection (mobile, wifi, etc). Given the increasing use of permanent connections on mobile devices, it is easy to see how more and more applications will use such protocols to stay connected - making one “internet connection record” which could even have passed the 12 month time limit by the time it is logged.

Connections are also typically encrypted and have some data passing all the time, so it would not be practical for an ISP, even using deep packet inspection, to indicate that the girl “accessed twitter” right before she vanished, or even at all (just that there is a twitter app on the phone and logged in).

It seems that even this emotive example is seriously flawed, and any arguments involving serious crimes unravel very quickly with the utter simplicity of using Tor, VPNs and secure messaging applications on devices these days. Yes, there are some stupid criminals, but it is getting harder to avoid using such services even without thinking about is as applications are increasingly moving to secure service provision so as to avoid threat from criminals. It has the side effect of also hiding from law enforcement.

Given that the examples given are already somewhat flawed, I feel the whole justification for trying to log “internet connection records” at all needs to be seriously reconsidered.

---

9 Use of web proxies

It seems that one of the main sources of Internet Connection Records, i.e. those which provide web site names, are likely to be from operators that use a web proxy. This is the case with many mobile providers. A web proxy was a useful tool in the days of dial-up Internet and slow connections in to the Internet - it provided a faster access for web sites and reduced transit costs. Mobile operators still use them to some extent, and some even rescale images to load faster on mobile devices.

However, with the advent of 4G and faster networking they are not only becoming obsolete, but actually a costly inconvenience. As such, it seems highly likely that operators will phase these out and hence stop providing this level of logging.

Again, this calls in to question the whole justification for logging “internet connection records”.

---

10 Carrier Grade NAT logs

Another obvious source of Internet Connection Records is the Carrier Grade NAT (Network Address Translation) boxes that are very common in mobile providers and starting to be used by some of the larger operators.

Basically these boxes allow for the sharing of IP addresses. As IP version 4 has run out, this is becoming necessary in many larger networks. They have the side effect that they may log many types of “session” or “connection” made across the network, and these logs can be retained as an “internet connection record”.

Whilst this does not offer web site names, it does provide IP addresses, and could perhaps be used to find that a phone has been connected to twitter 24 hours a day, for example.

However, CGNAT is relatively expensive, and deployment of IP version 6 makes it obsolete. With major services like google and Facebook already using IPv6, it will soon be the case that this source of connection logs will also disappear.

Again, this calls in to question the whole justification for logging "internet connection records".

11 Use of https

There is also an increasing trend within the industry to encrypt everything. Once confined to on-line banking, secure web sites are now being used for normal everyday business web pages. https is already extensively used by Facebook and google and many others, and over the next few years it is likely to become quite rare for a web site to be unencrypted.

At present some level of deep packet inspection can find the web site name of an encrypted web site from the initial negotiation, but this loophole is being plugged in the more modern protocols.

Again, this calls in to question the whole justification for logging "internet connection records".

12 The future of data retention

It seems clear that the retention of any sort of "Internet connection record" is of very limited use at present. The current proponents of this logging do not understand how the Internet works. Experience of Denmark for 10 years suggests that it is not useful. It is also clear that over time the availability of such logs and usefulness of the logs will diminish.

I feel that retaining data on web page and Internet services access is therefore not viable in the long term, of limited use now, and not proportionate in terms of costs or privacy, so should be excluded from the bill.

In the long term I suspect that even call data records for telephone calls will become useless as people use more messaging applications and secure voice and video calling.

13 Data Protection

It is not clear if retained data is subject to a Data Protection Act Subject Access request, or related requests to correct such data.

This needs clarifying.