Investigatory Powers Bill

Written Evidence

Adrian Kennard
Director, Andrews & Arnold Ltd, an ISP
Director, FireBrick Ltd, a firewall/router manufacturer

Summary

This is a hugely important Bill and there are key issues that need proper parliamentary debate.
It proposes new powers which have serious technical, moral and human rights issues.
It also addresses the continuation of existing powers which have never been debated in Parliament before which should not simply be re-enacted without clear justification.

Key points regarding the Bill are highlighted with bullet points. At the end of this document I have proposed specific amendments to the drafting of the Bill for some of these points.

Of particularly difficulty is the concept of *content* vs *communications data* which is key to many parts of the Bill.

Overview

The Bill aims to consolidate and formalise existing powers of the intelligence services, and existing data retention powers, as well as “simply” extending retention powers to cover *Internet Connection Records*.

Even these simple objectives need to be considered carefully.

The powers of the intelligence services were made clear by Edward Snowden, and the reaction of the world has varied. Public are outraged, and countries such as the US have backed down on their surveillance of their own citizens, yet the UK plans to strengthen the legal basis for these powers and continue to use them.

The EU regulations for retaining data were quashed by the EU, but the UK’s reaction was apparently not to see these as the invasion of privacy that they are but to enact a continuation of these powers, and now to try to extend these powers into much more pervasive invasions of privacy.

The Bill deliberately combines the powers of the Intelligence Services and the powers for more *day to day* police work. I feel that this is causing a lot of confusion for the public - my own experience is that there are many people who may well be in favour of the Intelligence Services *keeping us all safe* but do not appreciate the many different powers provided by parts of the Bill.

- The wording of the Bill should make these two purposes much clearer and distinct

Overall the Bill has far too much secrecy - with gagging clauses in almost every section. These powers have caused public outcry and have been disclosed by someone taking great risk and breaking laws to expose the truth. It is clear that where such powers do notes actually require secrecy for justice to be served, then these powers should not be conducted in secret.

- Secrecy and gagging clauses should all be reviewed and changed so that they only apply where absolutely necessary, and only for as long as it is absolutely necessary, thus allowing public visibility and scrutiny of these intrusive powers on an ongoing basis.
- The secrecy clauses are inconsistent with many of them not even allowing disclosure to legal representatives. The secrecy clauses that remain should be made more consistent.

Existing powers

The powers that the Intelligence Services use already have come as a surprise and revelation to the public and even to MPs. Though these are deemed *legal* under existing legislation, albeit by secret and perhaps *creative* interpretations, that does not mean that these powers should be *rubber stamped* into new law. These are powers that have never been properly debated in Parliament and they should be now.

- I feel strongly that if the current parliamentary timetable for this Bill does not allow proper debate of these existing powers then this part of the Bill should be removed, leaving those existing powers in place under existing law until such time as they can be properly debated.

These proposed powers are excessively intrusive and are nothing less that *spying on our own people*. The Home Office needs to make a clear operational case for these powers. Fortunately, as they are existing powers and in use the Home Office should be able to not only provide a clear *operational case* for each power, but should be able to provide actual detailed examples of how each power has been effective and proportionate in their purpose in the past.

Even so, I have made more detailed comments below on aspects of those existing powers if the Bill is to retain them.

New powers

The Bill purports to add *Internet Connection Records* to existing data retention powers. However, even where the clauses in this Bill are verbatim copies from existing legislation the meaning and extent of the powers has changed because of important changes to definitions. As a simple example, previous powers in many parts of the Bill only applied to *Public Communications Operators*. The new definitions extend these powers to private networks such as JANET, to office networks, and even to home networks and equipment and software manufacturers. This is a massive change in scope which is buried in subtle changes to definitions.

- The justification for these changes needs to be made clear or the wording changed to restore the narrower scope of such powers if they are to be retained.
- The Bill should use a consistent set of definitions such as reference to the Communications Act, and should only apply powers to public communications providers.
- Equipment and software manufacturers should be explicitly outside the scope of the Bill.

Targeted powers

The Bill makes clear distinction between targeted powers and bulk powers. However, the targeted powers allow *thematic* warrants and orders which can cover a very wide set of targets.

- Targeted powers should seek to limit their reach as much as possible, with specific requirements to ensure the impact is not extended to innocent parties more than absolutely necessary. Perhaps even place limits on number of persons, premises and devices that can be included in any targeted order/warrant.

Equipment Interference

Equipment Interference has huge scope to cause damage to the operation of communications systems as well as the stated objectives of covert surveillance. It is immensely powerful and needs corresponding justifications and controls.

It seems clear to all that if we are to allow authorities to bug someone's home with audio and video, then that can only be justified where such a person is a suspected serious criminal and where a proper judicial process with a judge signing a warrant authorises such action.

However, equipment interference not only allows such invasive surveillance on no more than a general warrant from the home secretary, but allows much more. It allows bulk and thematic warrants which will perform such interference on innocent parties, rather than targeting only the suspected criminals.

- Equipment interference should only be permitted where targeted only at a suspect in serious crime where a judge authorises the interference and feels it is proportionate, necessary and effective.

Equipment interference has a massive scope to cause damage, and I feel strongly that the party doing the interference needs to be liable for that damage. Such damage may be both technical in terms of the work needed to identify and undo the interference performed, but also to reputation. If GCHQ hack a SIM provider, and that costs them millions of pounds, GCHQ should have to pay for that.

- The Bill should make clear that those ordering equipment interference are liable for the consequences of the interference, perhaps even requiring specific insurance to cover such consequences.

In order for the possibility of liability to exist there needs to be transparency. Equipment Interference is such a powerful tool that there should be clear scrutiny of the use of such powers.

- The Bill should provide that those ordering equipment interference must disclose details of the equipment interference to all parties impacted by that interference once the purpose of the interference is complete and there is no longer a risk of prejudice of any ongoing investigations.
- The Bill should require those ordering equipment interference to provide details of all actions they have taken, and assist in repairing and reversing the interference they have performed. This should include providing details of any vulnerabilities they have exploited so that manufacturers can rectify those vulnerabilities.
- The affected parties should be free to publicly disclose the details of the interference if they wish (once there is no longer a risk of prejudice of any ongoing investigations).

The Bill provides for conscripting persons to assist with equipment interference. This is a serious issue, as nobody should be conscripted into law enforcement. It is understandable that communications providers may wish to assist in such actions, and so should have the necessarily immunity for their actions in doing so, but conscription is not acceptable. It seriously undermines any trust between providers of communications services and equipment, and their customers. The secrecy around such orders means that providers cannot even credibly provide assurances to their customers. This is bad for commerce and we already see companies threatening to leave the UK as a result of this Bill.

- The Bill should make clear that no persons should be conscripted into assisting with equipment interference
- The Bill could *permit* persons to assist without any risk of prosecution or cost to themselves

Bulk data sets

The justification for bulk personal data sets is very unclear.

- Parliament needs to debate the need for this clearly and properly understand example use cases and operational justification for this power.
- The specific personal data sets required should be set out in a schedule on the Bill

Intercept capabilities

Interception is an important power in the investigation of crime. The old fashioned *phone tapping* that could be performed to monitor the telephone communications of a serious suspect in a crime has no doubt been very helpful for furthering criminal prosecutions.

The Bill allows for intercept capability orders which are massively more far reaching in their scope, not simply *phone tapping* but more intrusive powers.

- The Bill should clearly provide a definitive list of specific powers that are to be available, not simply by a selection of examples, and there should be clear operational cases for each power.

The Bill makes some comment on encryption (protection) of data, but this is worthy of a separate discussion (below).

Encryption

It is possible for data to be encrypted and for that encryption to be applied by the communicating parties as *end-to-end encryption*. This means that there can be no way for any other parties to access the meaningful content of that communication. This is a fact of life and mathematics and is not something that legislation can change. Even outlawing such encryption would not stop it being used, and would have severe consequences to normal commerce and trade. Also, there are ways to use encryption covertly where there are no means to prove it is in use. The Bill does **not seek to outlaw this type of encryption** which can, and will, be used by criminals and terrorists alike, thwarting attempts to access the content of their communications. **There is always a safe place for criminals to communicate**.

The Government have made it clear that they do not intend to weaken security. However, the Bill fails to make it clear whether communications providers (communications companies, equipment providers, or simply software providers) are permitted to offer secure communications services to their customers.

As worded now, the Bill lists merely as an example, that an order could required removal of encryption actually applied by the provider, if practicable. The Bill does not, however, restrict such orders to this case, and could, as worded now, still allow an order forcing a provider that does offer a service with *end to end encryption* to change the nature of what they offer so that it is no longer *end to end* at all. This is clearly unacceptable and undermines trust in providers.

This is also ineffective against criminals which can still deploy their own end to end encryption with ease, or make use of third party encryption provided by non UK actors or the open source community. Such powers serve only to undermine security and undermine products and services. Once again companies are already threatening to leave the UK over this.

- The Bill should make it clear that use of encryption is not illegal.
- The Bill should make it clear that any company offering an encrypted communications service which is designed such that the company cannot access the content of the communications,

may do so legally and without risk of interference. Prohibiting such communications systems would not stop criminals but would impede commerce and the basic human right to privacy.

It is worth noting that even in the US, the FBI have backed down from forcing Apple to compromise security.

Data retention

Data collection and retention is clearly a form of *mass surveillance*. It is a nonsense to suggest that this is not so because no human looks at the data. If we take that notion to its extreme it would allow for 24 recording audio/video in every room in every home, but somehow not be an invasion of privacy as nobody is looking at it. The key point here is the deliberate, state mandated, collection of data, not simply a matter of retaining data already collected for business purposes. Collecting extra data for the state to use is *surveillance*. There is a basic right to privacy, and that should only be broken in specific cases. There is a good argument that any form of data collection should be targeted, so that it only applies in the case of a court order in respect of a suspect in serious crime.

The distinction between *communications data* and *content* is a key part of the Bill, separating the controls involved in these processes. This distinction only makes any sense where the communications data is relatively benign and non intrusive to the privacy of individuals. This may have been true for simple itemised phone bills in the past but is clearly not true now. Collecting details of every web site used in a premises, or by a person, as well as details of every communication made by every device, is clearly a matter of collecting sensitive personal information to which one should be able to expect some right to privacy.

However, where communications data is required in a *targeted* way, the powers in part 3 allow this to be collected and reported. This means a retention power is not required at all for targeted collection of communication data.

- MPs should debate if state ordered mass data collection is valid at all, and whether it should only apply as targeted surveillance and hence a retention requirement is not needed.

The term “retention” sounds harmless enough - it implies a party has data and simply has to “retain” it for a period. To some extent the previous regulations did imply this in that they only applied to data *processed or generated* (without actually defining those terms).

The new Bill makes a number of key changes which impact even such simple logging and retention. A key change is the extension of “processed or generated” clause to include “obtaining”. This means that an ISP that does not provide email could be ordered to “obtain” data about emails as data passes through the ISP’s network (third party data) - an expensive process. This is also somewhat futile as even now many email (and other) data exchanges are encrypted *on the wire* which will stop ISPs snooping on such data unless they are the email service provider themselves.

Removing “obtaining” and clarifying “processed” would mean that, for example, email logs would be logged at the point an email service is provided (an email server which processes that data). It means that telephone call records would be logged at the point a telephone service was provided (a telephone system or exchange); even web logs where a web proxy is operated, as is often the case with mobile operators; in short, the very things that the Home office have indicated they want.

This is very important from a technical and implementation point of view. Where data is in fact *processed* by equipment then it is generally much more technically practicable to log that data.

Even then, this is not always the case, as sometimes the data processing is at such a speed that dedicated hardware is used to *process* addressing information in a way that does not allow full logging.

Expecting data which is not in fact *processed* to be logged is always much less practicable, and where possible is much more expensive and problematic.

The Government has clearly stated that they are not expecting *third party data* to be collected. The wording at present includes that option, with no clear justification and contrary to the code of practice.

- The Bill should only require obtaining and retaining communications data where a provider is "processing or generating" that data.
- The Bill should define "processing" in this context as where some equipment in control of the provider actively considers the data in some way and is not merely passing the data through the communications systems, and still only where practicable.
- The Bill should define that it applies where processing is done on equipment in the UK

Even with the caveats of the codes of practice and accompanying notes it is clear that Internet Connection Records represent a hugely intrusive and revealing set of data on innocent members of the public. This is data on our personal lives carried out in the privacy of our own homes even though we are not suspected of any crime. That is clearly an invasion of privacy and a risk of this legislation being deemed in breach of Human Rights.

- If Parliament considers general spying on people in their own home acceptable, and as such some level of general data collection and retention to be justified, it should clearly define exactly what data is to be collected and retained based on clear use cases for this.
- This could be as a schedule on the Bill which can be amended from time to time.
- This should be a clear technical definition of the data to be retained by the party processing that data.

Filter

The *filter* function specified in the Bill is still very unclear. It seems to provide very general and automatic top level search functions, and far from providing extra privacy, it removes layers of privacy allowing *fishing trips* with ease.

The very concept of the *filter* highlights the extent to which this data retention is actually *mass surveillance* and *spying* on the innocent public 24 hours a day.

If collection of such data was properly targeted then there would be no need for the filter at all.

- The filter should be scrapped, or
- The justification for the filter fully debated by Parliament first

Codes of practice

There are many cases where the Bill provides far reaching powers and wide definitions only to have these more narrowly applied in codes of practice.

There is no justification for this - if there is no operational case for the powers, which is clear if the codes of practice do not call on them all, then the face of the Bill should reflect that rather than allowing wide open powers that can be abused in future.

Codes of practice do not have to be followed and can be changed, whereas changing the Bill needs proper consideration by Parliament. For this reason we need the actual Bill to be clear on these points.

One of the key reasons for this legislation in the first place is because of the secret and *generous* interpretations of previous legislation with very vague clauses. This Bill should address that with clear and specific clauses.

- The Bill should be reviewed overall to ensure that it reflects the specifics of the operational cases and requirements of the codes of practice and not have general wide powers beyond what is required.
- Where sensible to do so - cases should be defined in a schedule to the Bill which can be amended in future to cater for changes in technology over time.

Costs

The Bill makes a number of obligations in many areas on innocent parties, such as Communications Providers.

The Bill is not seeking to *punish* communications providers, but seeking to compel communications providers to provide valuable *services* to the Intelligence services and police and other authorities. As such there is no justification for any expectation for those impacted by the Bill to make any financial contribution. State conscription to law enforcement is not acceptable. The communications providers are not guilty of any crime or moral wrongs, but are requested to provide a service, and like any service they should be **paid for that service**.

Indeed, those that provide services to the police, whether *toner for their photocopier* or *petrol for their cars,* are not even expected to provide such services at *cost price* but paid a normal commercial rate for providing such services.

- The Bill should provide that any parties compelled in any way to provide any services as a result of this Bill should be fully compensated for doing so.
- The Bill should allow payment for such services to be at a fair commercial rate just like any other services provided to the Intelligence Services or police or authorities.

Technical

I have omitted the bulk of technical aspects of the Bill from the above to try and make it clearer.

The main technical issues are:

- Data retention should only be for data *processed* (actively considered) or generated in the UK - this is of key importance as otherwise the work involved in obtaining *third party data* from a communications stream is prohibitively complex and expense. It is also increasingly pointless in light of the modern trend towards general encryption of all traffic.
- If sensitive personal data is to be kept for a year there are huge implications on the way that data is stored securely. This is made worse by a requirement for automated access as part of the *filter* or *information retrieval* requirements. It is inevitable that there will be data breaches as a result of this. These will be massively more problematic than things like the Ashley Madison breach as this provides the same data but on every *delicate* web site accessed by *everyone* using any of the UK's major ISPs as well as data on which bank people use, what on-line stores they use, and much more that is useful to criminals. The very requirement to retain this data in the first place needs to be considered in light of these huge risks.
- Use of Tor, VPNs, and end to end encryption, as used by MPs and Lords to protect their own privacy, can continue and will thwart most of the powers in the Bill when it comes to criminals, making it wholly ineffective and disproportionate in many cases.
- The whole issue of differentiating *content* and *communications data* is worthy of a separate section [see below].
- This level of logging has been tried before, in Denmark, with detailed logging at a TCP/IP level, and it was found to be ineffective. Why are we not listening to that experience?

Given that level of collection and logging has already been tried in Denmark, and now abandoned - it may be a good idea for the committee, or cross party group of MPs, to actually arrange to visit the Danish officials and discuss their experience with this type of law.

Content vs Communications Data

The distinction between *communications data* and *content* is not at all clear. This is not simply because of the wording in the Bill, but because of the way the Internet works.

It needs to be clear not just in *legal wording*, like "anything with meaning is content" but in a way that designers can make computers understand. **This is a technical issue, and one which is almost unsolvable. If you cannot make computers understand the difference then you cannot implement the Bill.**

The distinction that we see in the postal system between *outside of the envelope* and *inside the envelope* simply does not exist in the Internet. There are layers and layers and layers and the content is mixed with the meaning at all sort of levels. The best we can do is have some very specific technically defined terms in a schedule to the Bill to make it absolutely clear what is logged, as we had with the previous retention directives.

There are some key examples of why this is an almost impossible distinction to make. Apparently the Home Office have confirmed that a web site address like "*bbc.co.uk/news*" is two separate parts, with "*bbc.co.uk*" being the *communications data*, and "*news"* being *content* as it relates to meaning.

This has the problem that *"news.bbc.co.uk*" is also a hostname, and the "*news"* part is therefore meaning (i.e. *content*) and not *communications data*. What needs to be logged in that case is also just *"*bbc.co.uk". So somehow a computer has to understand that part of the hostname is *content* and part is *communications data*, and apply the different rules in the Bill accordingly.

To highlight some of the difficulty here - even just with the above simple example, what of *"skynews.co.uk*", or "*news.com*". What parts of those hostnames are content and not to be logged, and what is left if you remove them? Do we log "*sky[redacted].co.uk*" and "*[redacted].com"* or something else?

I know of no algorithm that could determine which part of a hostname is *meaning* (i.e. *content*) and which part is not (i.e. *communications data*). There is no way to actually implement the requirements of the Bill if a computer cannot tell!

Another example is proxy sites, where the final site you are contacting may well be *after the first slash* and considered content, but it is actually the site ultimately being contacted. This highlights some of the layered nature of the Internet. Can you tell what is *content* and what is *communications data* from a URL like https://proxy-nl.hide.me/go.php?u=1sOTvDpQC2PSbsLdNPVgbA%3D%3D&b=5&f=norefer ? That was the URL I used to access "www.bbc.co.uk" just now.

What of "www.samaritans.org"? Is that access to the "Internet service" called "Samaritans", or is "samaritans" considered sensitive personal data that goes to the very meaning of my communication?

What of sites like "*abortionadvice.com"* where the meaning of the communication is clear from the entirety of the hostname, and is also clearly of **a sensitive personal nature**, so clearly should be considered *content*.

- The bill needs to abandon Internet Connection Records, and (if retaining data at all) stick to clear simple technically defined data types like telephone call records.

Other concerns

Some specific points on clauses in the Bill for which I don't have suggestions for revised drafting.

21: Judicial review is a procedural test to which the Secretary of State is already subject, and far from any form of "double lock". Orders should be approved by a judge as a proper judicial authorisation considering the matter in full.

53(4): Provides some very general powers to order persons that are *capable of obtaining* communications data to carry out *any conduct* in doing so - this seems oddly broad and could perhaps involve ordering persons to break into premises or racks in data centres or other criminal acts.

53(7): This list is extremely general. Communications data as defined in this Bill can still be very personal and revealing and deserves the protections of the right to privacy afforded by Human Rights. This list of reasons is far beyond those normally accepted as justification for breaching those rights.

78(3): Why not just have (c)? For example, for (a), if the communication lasts for a month, is the data in question the start or end of that communication?

84: Does not allow disclosure to legal representatives, equipment vendors, industry bodies, etc.

218(7): Seems massively open and should be removed or more clearly defined.

218(8): Does not allow disclosure to legal representatives, equipment vendors, industry bodies, etc.

223(6): Needs clearer definition that can be implemented technically - sadly I don't have specific suggestions for better wording, but if retention/etc orders were to list specific types of data that are communications data, then this would help matters.

Proposed Amendments

These only cover some of the points I have made above where I can see some specific changes of drafting that would be clear and helpful.

27: add clause “State the specific purpose that is to be achieved by the warrant.”

Without this, how would the Secretary of State be able to assess if the warrant is proportionate to achieving that purpose. Similarly in other cases in the Bill.

78(8)(b): remove “obtaining (whether by collection, generation or otherwise),”

78(8): add: “In this context ‘processing’ means that equipment within the control of the communications provider and located in the UK actively considers the data as part of its operation, rather than simply passes on that data through the communications system.”

This is important to ensure that there is no requirement to collect “third party data” and so to be consistent with previous regulations as well as the code of practice.

78(8): add: “A technically clear description of the specific types of data to be [obtained, or] retained”

An order for “all data” makes no sense from a technical point of view. In order to comply, or even to determine practicability, the specific type of data needs to be specified. Obviously this should not include “obtained” if obtaining data is removed from retention orders.

80(4): append “, and has taken action in accordance with subsection (10)”

213(6): replace “never be nil” with “fully reflect all reasonable costs incurred”

This is consistent with the statements that the Home Office intends 100% cost recovery.

218(4): replace with “No person can be compelled by an order under this section to reduce the level of security provided by a communications system. In particular where a communication system provides ‘end-to-end encryption’ no person can be compelled to change the design or operation of the system such that it is no longer providing ‘end-to-end encryption’.”

The original wording of 218(4) seems to be an attempt to reflect the repeated statements by the Government that they do not wish to weaken security. However it was simply repeating the “technical feasibility” test already in 218(3)(c)&(d). This proposed wording makes the stated intention much clearer.

218(11): append “, but does not include manufacturers of equipment and software”

225(1)”destroy”: replace “impossible” with “beyond reasonable recovery”.

It is generally impracticable to make recovery of data actually “impossible” in most systems.

And finally

If there are any MPs on the committee, or anyone else reading this, that are concerned over their own private communications (for which there is even a section in the Bill), I can recommend installing *Signal*, an app available for both iPhone and Android, which allows messaging and voice calls that are end to end encrypted and which cannot be intercepted in the network under this Bill.

So do think how much this Bill is costing, and how simple it is for innocent people, such as yourselves, to bypass its measures. Then think about how easy it is for any criminal or terrorist to do the same, and ask yourself if that is public money well spent.