A quick overview of the draft Investigatory Powers Bill

Health warnings

This is based on a very quick review of the draft bill and recollections of discussions from consultation meetings on these topics. It may contain errors and inaccuracies and I'll happily correct things if you tell me what I have got wrong.

Food for thought / to help discussion, and based on what I found interesting. Neither complete nor legal advice. Written in my personal capacity.

Licensed under CC BY-SA 4.0.

Copy of the bill available at https://www.gov.uk/government/publications/draft-investigatory-powers-bill

Neil Brown

4th November 2015

draft_IP_bill@neilzone.co.uk

Revision 0.2

Introduction

The last few years have been rather choppy waters when it comes to obligations capable of being imposed on communications providers under a broad banner of "surveillance" or "investigatory powers". The *Digital Rights Ireland* challenge to the EU directive of data retention resulted in the swift enactment of the Data Retention and Investigatory Powers Act 2014 (and the associated Regulations) and, not long thereafter, an extension to the regime to provide a framework under which providers could be required to retain certain IP address resolution information by way of the Counter-terrorism and Security Act 2015. The *Davis*/*Watson* judicial review action resulted in s1 of DRIPA being disapplied as of the end of March 2016.

Today's draft bill thus represents a rather major reviewing of the framework in respect of surveillance powers and obligations pertaining to communications service provision.

What the draft bill covers

The draft bill covers a number of key areas of surveillance law:

- interception
- acquisition of communications data
- retention of communications data
- equipment interference
- oversight
- "bulk" data and capability
- changes to the "maintenance of capability" and the "national security" regimes

What the draft bill does not cover

The draft bill does not cover all parts of RIPA, and Parts II and III — surveillance and covert human intelligence sources, and investigation of electronic data protected by encryption — which look as if they will remain in force.

Definitional changes

There are a number of important proposed changes to the definitions relating to communications data.

Content

Perhaps the most significant proposed change is at s193(6) where, for the first time (as far as I can recall), the legislation attempts to define what is "content" of a communication.

"Content" according to the proposed definition, is data:

> "which reveal anything of what might reasonably be expected to be the meaning of the communication".

This becomes very interesting in respect of layered communications — the situation, for example, in which a subscriber of a broadband Internet access service from provider A makes use of an over the top communications services from provider B. Provider A is likely to generate traffic data in respect of its carriage of packets from the subscriber to the next hop it that packet's destination. Conversely, what is actually in the packets would, on a traditional analysis, be most likely considered the content of the communication.

However, as the subscriber is using an over the top communications services, elements of the content of that packet might be traffic data in respect of that service (the intended recipient, within the over the top communications services environment, of the communication) — these data do not relate to the "meaning" of the communication, but relate to its routing, albeit routing within a service offered by provider B not provider A. Indeed, "anything in the context of web browsing which identifies the telecommunications service concerned" is expressly not content.

(One might also be concerned that, if there is a definition of "content" and a definition of "communications data", there is the possibility of a gap between the two definitions, through which things might accidentally fall — it might be worth the addition of a "catch-all provision" to cover this eventuality, stating that anything which is not "communications data" is "content".)

Entity and events data

Second, s193 introduces the notions of "entity data" and "events data". "Events data", broadly, relates to a specific event on a telecommunications system, and "entity data" describes a person or thing, or an association between that person or thing and a telecommunications service or system.

s193(5)(c) also introduces a concept of "architecture of a communications system", a notion which is not within the current scope of RIPA, and which presumably relates to information about, for example, cell tower location and active element configuration — information to which there is no specific access power currently, requiring forces to rely on a production order under PACE 1984 or other similar instrument.

Interception

Judicial Commissioner approval

A major change to the interception framework is that of requiring the approval of a Judicial Commissioner, in addition to the approval of the Secretary of State.(s14)

Targeted examination warrant

A second change is the introduction of a new type of warrant: a "targeted examination warrant", which covers the examination of intercepted material obtained under a bulk interception warrant (of which more below).(s12(3))

What about encryption?

There has been a lot written in the past few days about the extent to which the draft bill will seek to ban, or else undermine, end-to-end encryption. The word "encryption" appears only once in the draft bill, by way of a reference to existing powers under Part 3 of RIPA, which is outside the scope of the present reform.

However, s189(4)(c) provides that obligations imposed by a "maintenance of capability" order may include "obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data". A "relevant operator" is one who provide "telecommunications services" —

note, not just "public telecommunications services". (See "maintenance of capability" for more discussion on this change.)

Requiring interception product to be delivered in the clear is not new: Paragraph 10 of the Schedule to the The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 sets out that this is one of the requirements which can be placed on an operator under a "maintenance of capability" notice, and it is limited to encryption "applied by the service provider".

It would seemingly not, on the basis, apply to encryption applied by third parties (e.g. an over the top communications services encryption), or users. A company which provided a service which offered end-to-end encryption might need to argue that it was the subscriber, not the company, which controlled the encryption (if, for example, it required the subscriber to generate the encryption keys, such as in the context of someone configuring VPN software embedded in their device). For an end-to-end encrypted service under the control of the operator, that argument might be more challenging to make.

Network / content filtering no longer interception (if it ever was)

There has long been concern that the operation of certain network filtering services might amount to an act of interception.

This is addressed in the draft bill at s33(2)(c), which provides that interception is "authorised" where it is carried out by or on behalf of a telecommunications operator for:

> "purposes relating to the provision of services or facilities aimed at preventing or restricting the viewing or publication of the content of communications transmitted by means of postal or telecommunications services."

Network monitoring and security / detecting attack payloads etc.

The draft bill clarifies that interception undertaken to maintain network security, including detecting threats to the network / system, and to customer devices, is authorised(s33):

> "anything done for the purposes of identifying, combating or preventing anything which could affect (a) the telecommunication system by means of which the service is provided, or (b) any apparatus attached to that system."

Maintenance of capability

The draft Bill, at s189, proposes to extend the "maintenance of capability" framework found currently in s12 of RIPA.

Currently, the framework provides that a provider of a public telecommunications service being offered to more than 10,000 subscribers can be required to maintain the facility to provide assistance in relation to interception warrants.

The proposals in the draft bill expand the scope of this requirement in two ways:

First, a "maintenance of technical capability" order would no longer just be limited to providers of "public telecommunications services" but merely "telecommunications services" (s189(2)(b)). In this way, a service which is not offered to the public may still be ordered to maintain capability — this might apply to hosted services offering communications to businesses, for example, or perhaps those running cloud-based communications services on behalf of businesses.

Second, the current regime relates only to interception capability. The draft bill extends this(s189(3)(a)), and would permit a maintenance of capability order to be served in respect of interception, and also in respect of satisfying equipment interference warrants, bulk warrants and obligations under notices or authorisations for obtaining communications data.

These orders do not appear to require prior approval by a Judicial Commissioner — perhaps on the basis that a further instrument is required to make use of these maintained capabilities.

Obtaining communications data

Powers to require a communications provider to obtain and disclosure

Replacement for the powers under s22(4) RIPA are contained within s46(4)(d) of the draft bill. These powers provide that "authorised conduct" in respect of obtaining communications data may include a notice to a telecommunications operator:

> "(i) whom the authorised officer believes is, or may be, in possession of the communications data to disclose the data to a person identified by, or in accordance with, the authorisation, or
>
> (ii) whom the authorised officer believes is not in possession of the communications data but is capable of obtaining the data, to obtain it and disclose it to a person identified by, or in accordance with, the authorisation."

A provider's duty to comply with a disclosure notice remains limited to that which is "reasonably practicable".(s50(3))

Internet connection records

See discussion below in terms of retention of Internet access records but, in terms of the access regime, limitations on authorisations to require the disclosure of "internet connection records" appears in s47.

"over the top communications services" communications data

New wording which is unlikely to please traditional communications providers appears at s46(5)(c), which provides that an authorisation:

> "may, in particular, require a telecommunications operator who controls or provides a telecommunication system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system."

Given that a definition of "content" has been introduced, limited to the "meaning" of a communication, communications data

relating to an over the top communications services would seem to be entirely within scope of this provision.

(The Home Office might well argue that this is nothing new, since an obligation under s22(4) of RIPA could extend to "any communications data", not just communications data of the service provider. It is, however, unlikely to be welcomed.)

Filtering

s51 appears to authorise the creation and operation of a centralised communications data filtering capability, perhaps akin to that promoted under the draft Communications Data bill, both for determining whether an authorisation should be granted, as well as for the "lawful, efficient and effective obtaining of communications data".

New criminal offence

s66 proposes to introduce a new criminal offence, which a communications provider would commit in disclosing to the subject of a communications data acquisition notice the existence of that notice.

It is not clear how this might interact with the s7 "right of access" under the Data Protection Act 1998, given that the draft bill would seem to make it a criminal offence to disclose such a notice, whilst s27(5) Data Protection Act 1998 provides that "the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information".

Retaining communications data

Data retention notices

s71 would permit the Secretary of State to impose an obligation on a telecommunications operator by way of a retention notice to retain communications data for up to 12 months.

Retention or generation?

Although the framework is entitled "retention", it is possible that a retention notice served on a provider could require them to

generate data — perhaps even re-configure their network or service to generate — for the purpose of retention.(s71(8)(b)) This was a much-disliked aspect of the draft Communications Data bill, and probably an element on which providers will have quite a lot to say.

Internet connection records

The word "weblogs", so disdained after the previous draft Communications Data Bill, does not appear in the draft bill.

Instead, the key part for retention of what has become known as "internet connection records" appears to be within s71(9)(f):

> "the internet protocol address, or other identifier, of any apparatus to which a communication is transmitted for the purpose of obtaining access to, or running, a computer file or computer program."

Restriction on authorisation of access to internet connection records appears at s46.

This appears to build on the revision made by s21 Counter-terrorism and Security Act 2015, which permitted the Secretary of State to impose on providers under a retention notice duties to retain "relevant internet data". Relevant internet data included data which:

> "may be used to identify, or assist in identifying, which internet protocol address, or other identifier, belongs to the sender or recipient of a communication (whether or not a person)."

However, under the CTSA, the data could not include data which "may be used to identify an internet communications service" used by a subscriber, whilst this seems to be expressly permitted under the draft IP bill.(s71(9)(c) and (d))

Internet connections records would not be available to local authorities.(s46(6))

Existing data retention notices

Existing s1 DRIPA retention notices are to be treated as retention notices under the new regime, for the duration of the proposed six month transitional period. (Schedule 8, paragraph 2)

Safeguards: general information powers

DRIPA is repealed in its entirety, including the safeguards provision at s1(6). Instead, s9 of the draft bill proposes to constrain the bases under which communications data can be accessed. This is done on two fronts.

First, s9(1) repeals certain provisions of legislation listed in Schedule 2: these powers cease to be available.

Second, s9(2) limits the exercise of general information powers which are not repealed, unless they involve a court order or other judicial authorisation (for example, a special procedure material order under PACE). "General information powers" is defined in s9(4) as being a power which does not deal specifically with telecommunications operators.

Equipment interference

Part 5 of the draft bill introduces a framework relating to "equipment interference", which is defined in s81(2) as "interference with any equipment for the purpose of facilitating the obtaining of communications, private information or equipment data.

Previously, equipment interference powers were contained within s5 Intelligence Services Act 1994 and the Police Act 1997, Part III. For the first time, the framework moves from one of authorising agency action to one of compelling providers to assist: s101 establishes a duty of providers to assist once served with a copy of an equipment interference warrant.

Combined warrants

s170 provides that certain warrants may be issued for a combination of capabilities. For example, to combine an interception warrant with a targeted interference warrant.

National security / s94 Telecommunications Act 1984

The draft bill repeals s94 Telecommunications Act 1984 (which permitted the Secretary of State to give binding directions to providers in the interests of national security), and replaces it with what appears to be a "s94 Lite" provision, at s188, called

"National Security Notices". (The repeal is contained within Schedule 9, Part 1, Paragraph 1.)

s188(3) provides that a National Security Notice may be used to provide "services and facilities" to intelligence agencies, dealing with an emergency under the Civil Contingencies Act or to provide what would seem to be specialised communications services or facilities:

> "require the operator to whom it is given—
>
> (a) to carry out any conduct, including the provision of services or facilities, for the purpose of—
>
> (i) facilitating anything done by an intelligence service under any enactment other than this Act, or
>
> (ii) dealing with an emergency (within the meaning of Part 1 of the 10 Civil Contingencies Act 2004);
>
> (b) to provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively. "

s188 would still permit the Secretary of State to give directions in the interests of national security, but it expressly precludes the taking of any steps the main purpose of which is to do something for which a warrant or authorisation is required under the draft bill.(s188(4))

These notices do not appear to require prior approval by a Judicial Commissioner, but are within the scope of the oversight regime of the Investigatory Powers Commission.

Oversight: the Investigatory Powers Commission

The draft bill would establish (s167) a new oversight body, the Investigatory Powers Commission, under the leadership of the Investigatory Powers Commissioner, staffed with Judicial Commissioners. Existing oversight bodies are abolished (s178).

The main functions of the new body would include (s169) keeping under review the exercise by public authorities of statutory functions relating to the interception of communications, the acquisition or retention of communications

data or equipment interference; functions relating to the disclosure, retention or other use of intercepted material, acquired or retained communications data, or communications, private information or equipment data obtained by means of equipment interference; acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service; and national security notices.

"Bulk" warrants and personal data sets

The draft bill covers not only targeted activities, but also activities performed in bulk.

Part 6: bulk warrants

Part 6 covers bulk interception, bulk communications data acquisition and bulk equipment interference. In each case, authorised by the Secretary of State, and requires approval of a Judicial Commissioner.

Part 7: bulk personal data sets

Part 7 requires a warrant for the obtaining, retaining or examining of a bulk personal data set, either for a class of bulk personal data sets of for a specific bulk personal data set.

"Bulk personal data set" includes electronic personal data on a number of individuals where "the nature of the set is such that it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions". (s150)

Such a warrant is to be issued by the Secretary of State, but must be approved by a Judicial Commissioner, other than in respect of a specific bulk personal data set warrant where there is an "urgent need" for its authorisation.(154(5)(e))

Judicial authorisation

There is an emphasis within the draft bill of a secondary (perhaps prior) approval of certain warrants by a Judicial Commissioner, in addition to approval by the Secretary of State.

For example, the Secretary of State may issue a targeted interception warrant if the decision to issue the warrant has been approved by a Judicial Commissioner, other than where the Secretary of State considers that there is an urgent need to issue the warrant.(s14)

~~One point which potentially stands out in respect of this is a small sub-section which sets out the obligations or behaviours of a judicial commissioner, at s169(3)(5).~~

~~This provision states that:~~

> ~~"In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to (a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom."~~

~~Although this may well be intended to refer to a Judicial Commissioner's handling of sensitive materials and the like, one might question whether — by accident or otherwise — it would act to prevent a Judicial Commissioner from declining to approve a warrant which is authorised by the Secretary of State under one of those three bases. Hopefully an oversight rather than an intentional backdoor.~~

[Edited: Hugo Landau has kindly pointed out that s169(7) disapplies s169(5) (wrongly noted above as s169(3)(5)) when "deciding whether to approve the issue, modification or renewal of a warrant or authorisation."]

Conversely, "judicial authority" is required for certain local authority communications data acquisition — this is different to the requirement to secure the approval of a Judicial Commissioner.(s59)

Privilege

The bill does not appear to offer much in the way of protection for lawyer/client communications. The only reference I can find to legally privileged information appears in respect of the development of a code of practice about the obtaining or holding of communications data, which must include "provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds legally privileged

information or relevant confidential information". (Schedule 6, paragraph 4)

Cost recovery

The draft bill does not guarantee operator cost recovery, but does provide (s185(1)) that the Secretary of State must ensure that arrangements are in force for securing that telecommunications operators and postal operators receive an appropriate contribution in respect of such of their relevant costs as the Secretary of State considers appropriate.

The draft bill makes clear (s185(6)) that different levels of contribution may apply for different cases or descriptions of case but the appropriate contribution must never be nil.