# The Investigatory Powers Bill: Impact on Local Authorities

by Sam Lincoln

This article is aimed at members of UK local authorities; it may have value for members of other public authorities but what I say may not apply to all readers.

It's a daunting task to encapsulate the effect of a 193 page Bill - supported by 29 guidance pages and 67 explanatory notes – into a blog short enough to hold your attention; but I'll do my best.

The first thing to emphasise is that the Bill is a draft and there may be changes. Do nothing to change current procedures and practices other than make anticipatory plans and to consider the points I raise.

I'll leave the discussion about the politics of bulk data collection, the acceptability of Internet Service Providers being required to retain data and the effectiveness of the so-called 'double-lock' process to others. Suffice to say that the Act, if published without change to the Bill, appears to provide a proper legal basis to enable what cynics may consider has been going on anyway. Objectors may claim that, like RIPA, it protects public authorities more than citizens.

The Bill has three aims:

- to bring together existing powers to enable relevant public authorities to obtain communications and the data about communications; making the powers and safeguards "clear and understandable";
- to "radically" overhaul the way these powers are authorised and overseen;
- to make sure that the powers are "fit for the digital age"; to "restore capabilities that have been lost as a result of changes to the way people communicate."

The Bill has 9 parts and I'll summarise the effect of each in relation to local authorities. To save copying lengthy legal content, I refer to specific sections so it might be worth having a copy of the Bill available or to print this article and read it with an electronic copy of the Bill available for reference.

***Part 1 – General Protections***

This part sets out offences in relation to the unlawful interception of communications and the unlawful obtaining of communications data (CD). It also abolishes various general powers to obtain communications data and in which equipment interference can take place.

A member of a local authority is not enabled to grant the interception of communications or to undertake conduct amounting to an interception (see s.15 of the Bill) without consent unless for lawful business monitoring (see Part 2). To avoid commiting a crime, it's essential that you and your colleagues understand the relevant definitions and meanings. I thoroughly recommend that you read s.3 and s.4 to understand the meaning of an interception.

In effect you are committing an offence if, without lawful authority or the consent of a person with a right to control the operation or system, you intentionally intercept any communication in the course of its transmission by means of a public or private telecommunications system or public postal service.

Interception includes modifying or interfering with the system or its operation and monitoring transmissions with the effect of making some or all of the content available to a person who is not the sender or intended recipient.

'In the course of transmission' is clarified and means any time when the communication is being transmitted and any time when it is stored in or by the system (whether before or after its transmission).

Section 4 clarifies that any communication broadcast for general reception may be intercepted without a lawful interception warrant. But do not discount the possibility that a RIPA Part 2 authorisation (directed surveillance or CHIS) might be appropriate if the relevant criteria are met.

For your information, to allow for concerns regarding so-called 'mass surveillance', s.5 introduces specific types of interception warrant:

- a targeted interception warrant (TIW);
- a targeted equipment warrant (TEW);
- a bulk interception warrant (BIW); and
- a bulk equipment interference warrant (BEIW).

Since members of a local authority are not enabled to authorise an interception of any type, you should know that even if a crime is not committed, the new Investigatory Powers Commissioner (IPC) may serve a monetary penalty notice on a person if the conditions set out in s.6(3-4) apply. Note that the penalty notice will be served against the individual and not the organisation.

Probably of more importance to you and your colleagues is s.8 which introduces the new offence of knowingly or recklessly obtaining CD from a telecommunications or postal operator without lawful authority. If found guilty you could be imprisoned.

***Part 2 – Lawful interception of communications***

There are two occasions when a local authority may conduct an interception without a Chapter 1 warrant:

- when consent has been provided by the sender or intended recipient. But in this scenario the conduct may not take place without a valid authorisation under RIPA Part 2 or RIP(S)A Part 2 (see s.32); or
- for lawful business monitoring (see s.34).

***Part 3 – Authorisations for obtaining Communications Data (CD)***

It is vital that you read and understand the definitions at s.193. New terms such as Entity Data, Event Data and Postal Data are introduced which help to determine what CD is. I appreciate that the definitions are very legal but you do need to get your head around them.

I do not find local authorities included in Schedule 4 (Table of authorities and officers) but s.57 confirms that a local authority is enabled to obtain CD but only if necessary for the purpose of preventing or detecting crime or the prevention of disorder and that the conduct authorised is proportionate to what is sought to be achieved.

A local authority authorisation to obtain CD may only be granted:

- by a designated senior officer who holds the position of director, head of service or service manager or higher;
- **after consultation with a person who is acting as a single point of contact (SpoC)** unless in exceptional circumstances such as a threat to life or emergency.
- **if the local authority is party to a published collaboration agreement certified by the Secretary of State** (s.63 sets out the requirements); and
- to a person who is an officer with a local authority which is a supplying or subscribing authority under a collaboration agreement.

My emphasis in bold highlights that these are new requirements. I suspect that they will not be changed so it would be wise to start preparations to prevent inhibiting investigations when the Act is published.

A local authority designated senior officer may not grant an authorisation for the purpose of obtaining data already held by a telecommunications operator and which is, or can only be obtained by processing, an internet connection record (see s.47(6)).

Each local authority authorisation must be approved by a judicial authority (as described in s.59(7)) and will not take effect until it has been approved. (Section 59 sets out the conditions for approval).

The conduct that may be authorised is set out in s.46.

Section 48 sets out the procedure to be followed. No significant change to the current practice of writing an authorisation which includes *specific* detail. I emphasise the need to specify because too often detail was missing in authorisations that I examined when inspecting public authorities. It is my contention that authorisations which lack detail should not be considered valid (but that's probably the subject of a later blog!).

Each authorisation lasts for one month and may be renewed at any time before it ceases to have effect. Note that the period commences at the time it is granted not at the time it is approved.

Section 65 provides similar protections to those provided by RIPA s.27 – namely that conduct that is in accordance with, or in pursuance of, an authorisation is lawful for all purposes. I would prefer that the word 'valid' precedes authorisation because an authorisation which does not meet the standards set out in legislation (particularly with regard to describing, specifying and articulating proportionality) should not, in my humble opinion, be regarded as valid. Just sayin'!

***Part 4 – Retention of CD***

This Part relates to the retention of data for 12 months by service providers.

For your purposes, it is wise to destroy all CD as soon as it is no longer required. When cancelling an authorisation, it is best practice for the Designated Senior Officer to provide express direction in this regard. Verifying in an auditable way that the direction has been followed is also best practice.

***Part 5 – Equipment interference***

A local authority is not enabled to apply for an equipment interference warrant.

***Part 6 – Bulk warrants***

A local authority is not enabled to apply for bulk warrants.

***Part 7 – Bulk Personal Dataset (BPD) warrants***

A local authority is not enabled to obtain bulk BPDs.

In essence there is no change to your current obligations in compliance with the Data Protection Act 1998.

***Part 8 – Oversight arrangements***

The Act will abolish the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Surveillance Commissioners combining them into a single body of Judicial Commissioners headed by an Investigatory Powers Commissioner (IPC).

His main oversight functions are set out in s.169 and include all of the functions of his predecessors. But there is an interesting set of clauses (ss.5-7) which my legal contacts tell me is unusual. There is specific direction relating to what a Judicial Commissioner may not do. This is not an appropriate place to discuss this but some might say the direction interferes with judicial independence and encourages Judicial Commissioners to back off when it is claimed that their inquiry interferes or inhibits operations. I cannot envisage a scenario when a local authority would be so bold!

In my capacity as an ex-inspector, I am disappointed that a Judicial Commissioner may not keep under review the exercise of any function by a judicial authority (s.169(4)(b)). Since a judicial authority includes any JP, it suggests that the IPC may find it difficult to comment on the performance of those who approve local authority authorisations. My concern is that JPs who approve inadequate authorisations undermine the standards properly set by the oversight body. In my opinion, JPs must be encouraged to undertake relevant training.

You should note that the IPC will have - in addition to providing approval, audit and inspection functions - a duty to conduct investigations and to inform individuals who have been subject to serious errors by public authorities. However, the IPC and Investigatory Powers Tribunal (IPT) must agree that the error is serious and that it is in the public interest for the person concerned to be informed. I doubt that there will be many instances which meet the exacting conditions but you should be aware that a public authority must be asked to make a submission to the IPT if an error report is contemplated. However, all errors (whether or not reported to the person concerned) will be included in an Annual Report made available to the public.

Section 175 imposes a duty on all public authorities to report to the IPC -

- any refusal by a telecommunications or postal operator to comply with an authorisation; or
- any relevant error of which it is aware.

***Part 9 – Miscellaneous and General Provisions***

I find nothing in Chapter 1 of this Part which, in my judgement, directly affects a local authority.

In Chapter 2, s.193 to s.195 provides definitions of terms used in the Bill. It's always worth studying these to make sure that terms are used accurately.

Section 196 makes clear that individuals as well as organisations may be liable to be proceeded against and punished.

***Summary***

I hope this examination of the Investigatory Powers Bill has been useful. I may have missed something so advise your legal department to read the Bill if it hasn't already. When it's passed as an Act I'll let you know if there are any significant changes. In the meantime, encourage your leadership and colleagues to plan for the changes currently proposed.

When the Act comes into force I'm sure that the Act Now team will put together relevant training. To help make sure that this training is exactly what you want, why not send us your questions and requirements ahead of time so that we can start thinking about the best delivery method and products for you. If you think I've missed something important or wish to comment please feel free to do so – we can learn together!

Disclaimer: Any opinions expressed are those of the author alone. The article is not to be construed as legal advice – always seek professional legal advice if in doubt.

***Sam Lincoln was formerly Chief Surveillance Inspector with the Office of Surveillance Commissioners (OSC) for seven years. Sam has designed our RIPA E Learning Package which is an interactive online learning tool ideal for those who need a RIPA refresher before an OSC inspection.***