Investigatory Powers Act 2016 becomes law

Date : November 29, 2016

What is the Investigatory Powers Act?

The Investigatory Powers Act 2016 (sometimes known as the IP Bill before it became law) is new legislation aimed at helping the UK Government have access to data to fight terrorism and other crimes. It does however have wider ramifications – even the introduction to the IP Act calls it:

"*An Act to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.*"

It's a long piece of legislation with 176 sections stretching to around 304 pages in the current version.

We use some technical terms in this glossary some of which are explained here.

Where is the legislation currently?

There was a race against time for the Government as they wanted the IP Act to become law before the existing data retention legislation, the Data Retention and Investigatory Powers Act 2014 (DRIPA) expires on 31 December 2016. DRIPA is a time-limited law – it will expire unless renewed or replaced.

Outstanding issues on the IP Bill were resolved on 16 November 2016. It received the Royal Assent today. Different parts of the Act are likely to come into force on different dates – exact details are awaited but some parts of the law are in force now and we expect some additional provisions to be in force from January 2017. Again this is quite complicated – s.272 of the Act has more detail on this.

What's the history?

The draft Bill was published in November 2015.

Theresa May, the current Prime Minister and former Home Secretary has been a longstanding proponent of this legislation.

DRIPA has been well-used. Home Office figures show there were 517,236 authorisations in 2014 of requests for communications data from the police and other public bodies as a result of 267,373 applications. There were 2,765 interception warrants authorised by ministers in 2014.

What are the key elements of the IP Act?

Much of the new law is focused on access to Internet Connection Records (ICRs). ICRs are records of the internet services that have been accessed by a device – essentially a log of the device's activity. ICRs would include, for example, a record of the fact that a smartphone had accessed a particular social media website at a particular time.

The IP Act has a number of different elements including:

1. bulk interception
2. bulk acquisition of communications data – the law requires communications service providers (CSPs) to store ICRs visited for 12 months for access by police, security services and other public bodies. The obligation is to store ICRs but not the particular pages and not the full browsing history.

3. bulk equipment interference – the law gives the security services and the police the ability to access and bug computers and phones. It also places a new legal obligation on companies to assist in these operations to bypass encryption.
4. anti-tipping off provisions

ICRs can be accessed:

1. To identify the sender of a communication. This could be used for example to locate the particular device from which an illegal image was uploaded to a website at a particular time.
2. To identify the communications services a person is using. This would for example allow the police to determine whether a missing person was using a particular smartphone app or social media website prior to their disappearance.
3. To determine whether a person has been accessing or making available illegal material online.

The new law does have some extra-territorial reach although providers outside of the UK have less responsibilities.

The law undermines legal professional privilege, however not to the extent first proposed after lobbying from The Law Society and others. There is more about this in the links below. Criticism remains however of the new law's affect on privilege. The Chairman of the Bar Council, Chantal-Aimée Doerries QC said at the end of November "*sadly what was passed in the end fell significantly short of what we would consider sufficient to protect this important and fundamental right, underpinning the rule of law*".

It is important to remember that a lot of the IP Act is not new – many of the powers in the IP Act are carried over from DRIPA.

There has also been longstanding opposition to the IP Act by the trade union movement who believe that the new legislation gives law enforcement and the security services greater powers to access trade union data and also undermines the ability of journalists to protect their sources.

Who can exercise powers under the IP Act?

It is important to remember that the powers in the new law are not just limited to the security services and to the police. Other bodies are given powers including:

1. HMRC
2. the Department of Health
3. the Food Standards Agency
4. the Gambling Commission
5. the Department for Work and Pensions
6. the Department for Transport
7. local councils
8. the Competition and Markets Authority
9. the Financial Conduct Authority
10. the Gangmasters and Labour Abuse Authority
11. the Health and Safety Executive
12. the Information Commissioner's Office (ICO)
13. the Serious Fraud Office

Not all of these bodies are given the same powers.

Does the Act outlaw encryption?

No. The new law includes an existing power to compel a company in the UK to hand over an encryption key so that encrypted messages can be read - where there is a legal reason for the police or other agencies to access that message. However, this legal duty cannot be imposed on overseas companies.

Are there any safeguards?

The new law sets up a new supervisory body, the Investigatory Powers Commission or IPC. The IPC will be lead by a senior judge appointed by the Prime Minister. S.227(2) emphasises that the Investigatory Powers Commissioner must hold or have held "*high judicial office*". As an indication of the likely calibre of IPC appointees the current Interception of Communications Commissioner is The Right Honourable Sir Stanley Burnton, a former Court of Appeal judge.

The law does contain some checks and balances including a new "double-lock" on ministerial authorisation of intercept warrants with power of veto. However exemptions are allowed in "*urgent cases*" of up to five days. If the IPC finds a serious error in how powers have been used, the Investigatory Powers Tribunal, a special court, could then rule that the targeted individual has the right to know.

While local councils can request some communications data, they will be banned from accessing internet connection records.

The Prime Minister is to be consulted in all cases involving interception of MPs' communications. Safeguards on requests for communications data in other "sensitive professions" such as journalists are written into law.

The ICO will have audit powers.

One of the issues with the old legislation however was its over-use for relatively petty matters by junior functionaries. We have had issues for example with the attempted use of DRIPA and other powers by housing benefits agents and low-ranking HMRC officials who have felt themselves to be above the law. This is despite the fact that some of the existing legislation, like the IP Act, has a seniority threshold for requests. It is to be hoped that the clarification of their powers in the IP Act will also be accompanied by proper training to make sure that these powers are used as a last resort rather than as the first option for lazy officials. Whether that turns out to be the case however remains to be seen.

Will it be challenged?

The IP Act could be affected by the outcome of the pending legal challenge to DRIPA. This was brought by David Davis MP (who has now dropped out following his ministerial appointment as Secretary of State for Exiting the European Union) and Tom Watson MP, the Deputy Leader of the Labour Party. A decision of the European Court of Justice is likely soon. If the European Court of Justice was to follow the Advocate General's Opinion, some aspects of the IP Act would be in conflict with EU law. If that were the case further challenges would seem likely.

In addition on 28 November the UK Parliament announced that it had received 118,000 signatures on a petition asking the UK Government to repeal the new law. This means that the petition will now be considered for parliamentary debate. The law does continue in effect whilst this debate is scheduled however.

Will this matter post-Brexit?

Whatever the situation after Brexit the UK will still have obligations under human rights legislation. In addition the IP Act is likely to make it more difficult for the UK to pass any adequacy test which is important for transfers between the EU and the UK. This is likely to be on the agenda of many including privacy activist Max Schrems who talked about this in our interview in October.

What should businesses do?

The response for business will depend on the nature of their operations. CSPs will obviously need to pay closer attention to the law than other businesses however every business needs to review the way in which it handles requests particularly given the increase in Subject Access Requests and Right To Be Forgotten Requests in recent years which we have written about here. This volume is likely to increase once GDPR comes into force on 25 May 2018 (see our GDPR FAQs here). It is likely that once the IP Act comes fully into force we will see a significantly

increased number of requests being made but also more attempts to scrutinize what is happening with their data from data subjects.

Jonathan Armstrong and André Bywater are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

There are more materials on the Act on Parliament's website here.

The Law Society's response is here.