

# **Electronic Surveillance: a (not so) brave new world?**

**Michael Drury** and **Luke Clements** consider the public response to the Investigatory Powers Act 2016 and the ensuing debate surrounding internet connection records.

## **The Investigatory Powers Act 2016 receives Royal Assent**

The Investigatory Powers Act 2016 (IPA) – known colloquially as the “Snooper’s Charter” – has been one of the most hotly debated laws of recent times. The product of Theresa May’s tenure as the Home Secretary, NGOs and opponents now suggest there was insufficient scrutiny given by Parliament during its passage.

Weighing in at almost 300 pages and comprising of 272 sections, ten Schedules and six detailed draft Codes of Practice, it is by no means a simple piece of legislation. However, after almost a year of debate, and a swift passage through its final Parliamentary stages, the IPA received Royal Assent on 29 November 2016 and has now become law. But, what does it do – and aside from the effect of court challenges to the existing law (see our separate commentary on *Watson*) – what are the issues now arising?

## **Background**

The IPA was introduced in response to heightened criticism of the surveillance activities undertaken by public authorities in the UK. This was at a time when the Snowden revelations, and the litigation that ensued, had led to an outcry by NGOs and interest groups as to the Government’s collection and use of communications and communication data.

When drafting the IPA, the Government sought to codify the existing laws governing data monitoring into one single legislative scheme. The aim of doing so was to ensure that public authorities, particularly law enforcement agencies and the security and intelligence services, had powers that were not only fit for the digital age but also human rights compliant.

## **The public response**

Notwithstanding the (eventual) Parliamentary consensus, what has been remarkable is the negative public reaction to the IPA passing into law. This is most apparent in relation to the introduction of powers relating to internet connection records (ICRs), which have been the topic of much of the dissatisfaction surrounding the IPA.

To illustrate the public discontent, a petition to repeal the IPA, posted on Parliament’s website, has garnered over 206,000 signatures; this is unprecedented in respect of new legislation. Unsurprisingly the Parliamentary Petitions Committee decided not to hold a debate on this petition, citing the fact that the IPA had previously been debated on many occasions and had already been the subject of scrutiny by an expert committee. Nevertheless, the sheer number of signatories to the petition reflects a potential post-Brexit shift in social attitudes, whereby the public are now more willing (and eager) to come together to challenge the legitimacy of decisions made under the aegis of democracy, particularly when a decision has the potential to impact on their human rights or freedoms. In a further display of discord, human rights campaign group, Liberty, has started a crowdfunding appeal to underwrite a judicial review of the IPA. The appeal has quickly

reached its initial target (over £50,000 in donations) and continues to gain momentum. In a time of austerity, this level of support is striking and should not go unnoticed.

### **Internet connection records – not all they are cracked up to be?**

Powers relating to ICRs are one of the most – if not the most – contentious aspects of the IPA. For many, the retention and disclosure of ICRs are seen as excessively intrusive and out of sync with human rights obligations.

Broadly speaking, an ICR is capable of constituting a range of data showing: **when** a connection was made; **where** a device was located when making the connection; **what** service a device accessed; and **who** made the connection i.e. what device was used. However, as a matter of law an ICR will not show what an individual did on a particular website. This means that public authorities that acquire ICRs will be able to see that a device accessed a given website on a specified day, but an ICR will not show the images, content, communications etc. that were accessed using that website.

This does little to dissuade some critics, who argue that the collation and retention of such data is still grossly invasive and open to exploitation. In some respects this opposition is justified; the websites we visit have the potential to disclose deeply personal information about us. Whether it relates to health, addiction, infidelity or sexual preferences – to name a few – there are many who would rather keep such information private and out of the hands of the Government (or, worse yet, the hands of hackers).

The limited nature of ICRs also presents an issue for public authorities – particularly law enforcement – who will undoubtedly be left to question their usefulness as an essential investigative tool. It will be an uphill struggle to build an accurate picture of an individual's online activities without knowing what the individual did on a given website. This is most prominent where ICRs are obtained for the prevention and detection of criminal activity. In this case, it is of limited use to know that an individual visited a particular website (albeit potentially one that is unlawful in its content). Instead a public authority will want to know what the individual did on the website, what images were uploaded or downloaded, or what posts were made.

### **Conclusion**

The enactment of the IPA has already commenced, with the data retention provisions having come into effect on 30 December 2016. We assume it is only a matter of time before the Home Secretary uses her discretionary powers to bring the remaining sections into force, although there seems to be no obvious urgency. However, given the breadth of criticism of the IPA, one is left to wonder whether the Government would be so attached to the Act had the current Prime Minister herself not invested so much personal capital in its success.

**Michael Drury & Luke Clements**

**BCL**