The Investigatory Powers Act 2016

Weighing in at 291 pages and comprising 272 sections, 10 Schedules and 6 detailed draft Codes of Practice, the Investigatory Powers Act 2016 (IPA) (which received Royal Assent on 29 November) passed its final Parliamentary remarkably quickly. Praised by the Government as *"world-leading legislation that provides unprecedented transparency and substantial privacy protection"*, the IPA has been condemned by privacy campaigners for licensing "*the most extreme surveillance in the history of western democracy"* and for representing *"a beacon for despots everywhere".*

Notwithstanding the fierce extra-Parliamentary criticism, the relatively muted opposition from MPs and peers reflects in part the fact that, in many areas, the statute merely codifies and makes more transparent existing laws governing data monitoring by the police and intelligence services in the UK. In some respects, however, when the IPA is brought fully into force, it will legitimise controversial pre-existing surveillance practices. Nevertheless, it looks certain to be challenged in the ECJ and ECHR at an early stage.

Pre-empting such challenge, the IPA aims to navigate a path through European and human rights jurisprudence to create a comprehensive scheme for the use of powers by UK public authorities to obtain communications and communications data (i.e. the "who", "when", "where" and "how" of a communication but not its actual content), not only from within this country but from elsewhere. Affecting telecommunications operators (broadly, any entity offering, providing or controlling facilities for using a telecommunications service in the UK, including social media providers) the IPA regulates six main areas of activity:

1. Ensuring technical capability for effective interception and surveillance (including de-encryption);
2. Interception warrants;
3. Retaining communications data (for example everyone's internet connection records).
4. Obtaining communications data;
5. Equipment interference (hacking);
6. Processing bulk personal data sets (in other words large lists containing the names of many people, most of whom are of no interest to the authorities, for example everyone with a passport or a licenced firearm).

Ensuring Technical Capability for Effective Interception & Surveillance

To ensure that the powers within the IPA can effectively operate, the Act provides for the issuing of confidential Technical Capability Notices (TCNs) to telecommunications operators. A TCN will oblige recipients, whether based inside or outside the UK, to take all steps specified within the TCN.

Before issuing a TCN, the Secretary of State must consult with the proposed telecommunications operator recipient and must be satisfied as to the TCN's necessity and proportionality. Prior approval must also normally be sought from a Judge in the form of the newly established Judicial Commissioner.

On pain of civil injunction, telecommunications operators, whether located in the UK or abroad, will be under a duty to comply with a TCN, though it must be reasonable for the telecommunications operator to comply with its requirements.

Echoing the de-encryption dispute between the US Government and Apple in early 2016, TCNs can oblige telecommunications operators to remove or weaken electronic protection applied by them to communications or data. Quite how this affects "end-to-end" encryption applied not by telecommunications operators but by the senders and recipients of communications is as yet unclear.

Interception Warrants

Activities such as listening to electronically transmitted conversations or reading the contents of electronic messages, permitted on the grounds of national security, prevention and detection of serious crime and for the UK's economic well-being, will be governed by the IPA's provisions for specific/targeted and bulk interception.

Provided certain preconditions are met, the Secretary of State may issue warrants authorising such interception to persons both inside and outside the UK, though where the recipient is a telecommunications operator outside the UK, there will be a duty of prior consultation before any decision to issue.

Subject to what is reasonably practicable, recipients of interception warrants must take all reasonable steps to give effect to the warrant, irrespective of whether or not they are in the UK, and the IPA provides for both penal and civil sanction to reinforce this duty. The costs of compliance with an interception warrant are mitigated by an "appropriate" contribution from the Government.

Retaining Communications Data

In order to ensure the availability of relevant communications data to law enforcement and the intelligence and security services, the IPA provides for 12-month data retention notices issued to UK and overseas telecommunications operators. Before such notices are issued (on the grounds of national security, preventing or detecting crime, preventing disorder or ensuring financial stability), matters such as necessity, proportionality, technical feasibility and the cost of compliance must be taken into account, and reasonable steps must be taken to consult with the telecommunications operator on whom they would be served.

Of course, similar provisions relating to data retention and access pre-existed the IPA, and indeed in *Watson & Ors* they had already given rise to litigation before the ECJ with regard to their compatibility with privacy and data protection. Nevertheless, with increasingly sophisticated and large-scale "hacks" by criminals and hostile foreign states, the vulnerability of stored communications data (which includes internet connection records (ICRs) – broadly information showing when and where a connection was made, to what service and the person who made it) has led to particular criticism of the IPA. Where an individual's ICRs betray a particular vulnerability (for example, frequent visits to online gambling or mental health websites), unauthorised access to someone's ICRs risks exposing

individuals in positions of influence to blackmail. Of course, how real that prospect is remains unclear. Recent incidents – TalkTalk and Yahoo spring to mind – do not suggest 100% confidence is possible. However, the wider question remains: what would be the imperative for a hacker to access such information?

Obtaining Communications Data

Once retained, communications data (including ICRs) may be accessed either by a targeted authorisation warrant or a bulk acquisition warrant.

Targeted authorisation warrants, granted not by the Secretary of State but by a senior officer of the relevant public authority (from the police and National Crime Agency to the Department of Work and Pensions and Food Standards Agency), permit the obtaining of specific data relating to a particular operation. UK and overseas telecommunications operators receiving a targeted authorisation warrant must take reasonably practicable steps to comply, failing which they risk civil enforcement proceedings. In order to facilitate public authority access to communications data, the Government intends to create centralised software to enable queries across multiple databases, although it is understood that such software faces technical issues which may prevent its roll-out for the time being.

Bulk acquisition warrants are issued by the Secretary of State rather than senior officers of a public authority. Broadly, they may be issued where necessary and proportionate on the basis of national security, the prevention or detection of serious crime or in the UK's economic interests. The issue of a bulk acquisition warrant will normally be subject to prior approval by the Judicial Commissioner and can only be sought by the intelligence and security agencies.

Bulk acquisition warrants may be issued to both UK and overseas telecommunications operators, who must then take all reasonably practicable steps to comply, though the only sanction is civil enforcement, and even then, only against UK telecommunications operators.

Equipment Interference

The IPA provides two types of warrant for equipment interference (essentially the covert access to a device, system or network, for example the installation of spyware and monitoring of communication in real time): targeted and bulk equipment interference warrants.

The statutory regimes governing both types of warrant are essentially similar, including necessity, proportionality and prior approval by the Judicial Commissioner. However, targeted equipment interference warrants need not be sought on the grounds of national security, and may be sought by a wider range of officials than bulk equipment interference warrants which must always be sought on the grounds of national security by the head of an intelligence service. Unlike targeted equipment interference warrants, bulk equipment interference warrants are primarily aimed at overseas related communications, information and equipment. Subject to reasonable practicability, all telecommunications operators,

whether based in the UK or overseas, have a duty to comply with the provisions of such warrants, although the IPA makes no provision at all or enforcement action against overseas telecommunications operators, and only civil enforcement action is possible against those in the UK.

Processing Bulk Personal Data Sets

Bulk personal data sets (BDPs) comprise the personal data of a large number of individuals, which is held electronically by a UK intelligence service. Examples of BDPs include the electoral roll, telephone directories and travel-related data. If it does wish to retain a BDP, a warrant must be sought from the Secretary of State who, before issuing one, will consider whether it is necessary and proportionate and that there are satisfactory arrangements in place for storing the BDP and protecting it from unauthorised disclosure. A Judicial Commissioner must also give prior approval for the issue of a BDP warrant.

The IPA makes no provision obliging someone to make a BDP available to the intelligence services, though it seems the expectation is that requests would be acceded to on a voluntary basis, where necessary relying on the protections afforded for such disclosures under the counter terrorism and data protection legislation.

Overseeing the IPC Regime

As well as introducing the requirement for judicial approval for many types of warrant issued under the IPA, the legislation also provides for an independent Investigatory Powers Commissioner who will seek to ensure compliance with the statutory regime and who may be approached by telecommunications operators for advice and guidance about the operation of the IPA.

In addition, the Investigatory Powers Tribunal (IPT), which already exists, will continue to investigate and determine complaints against public authorities in relation to the operation of the IPA, with a new right of appeal from the IPT to the Court of Appeal.

Conclusions

Save for the data retention provisions which will come into force on 30 December 2016, the IPA's provisions will not be commenced for the time being. Clearly, significant preparation is required to enable the Act to operate efficiently. Notwithstanding this, and despite the safeguards which the Government has tried to incorporate into the IPA, the anticipated ECJ judgment in *Watson & Ors* is likely to have an impact on aspects of the legislation, and campaigning groups are threatening further legal challenges to the surveillance regime which the new legislation will govern. In the meantime, those likely to be affected by the IPA's provisions would be well advised to make themselves aware of the forthcoming measures as well as the practical steps which they might be asked to take as a result of the UK's new surveillance regime.

Michael Drury & Julian Hayes