Dr Ansgar Koene is a Senior Research Fellow at Horizon Digital Economy Research (http://www.horizon.ac.uk). Horizon is a Research Institute at The University of Nottingham and a Research Hub within the RCUK Digital Economy programme. Horizon brings together researchers from a broad range of disciplines to investigate how digital technology may enhance the way we live, work, play and travel in the future. Within Horizon, Dr. Koene has been working on the ESRC funded CaSMa (Citizen-centric approaches to Social Media analysis http://casma.wp.horizon.ac.uk) project which aims to promote ways for individuals to control their data and their desired level of privacy, including mechanisms that make it realistically possible to implement a withdrawal of consent. Indeed, one of the core CaSMa objectives is to ensure that social media users are aware of how their personal data can be used to understand human behaviour and the ethics of handling human data obtained from social media. ‘Citizen centric approaches’ refers to tools and methods that are sensitive to the personal nature of human data. Approaches that are ‘ethical by design’ with intrinsic transparency and dependence on explicit consent from the person who’s data is being analysed. Part of this work has included CPD seminars for SMEs, public engagement activities at the Web We Want festivals in 2015 (http://webfoundation.org/our-work/projects/web-we-want/) and collaboration with the iRights (http://irights.uk) coalition.

EXECUTIVE SUMMARY

1. Summary of function and need for IPB
2. Mandate of proposed judicial oversight
3. Concerns regarding proposed appointment procedure for judicial oversight
4. Key areas of concern expressed by industry and civil rights organizations
   4.1. Implications for customer trust and independent monitoring by journalists/civil rights groups
   4.2. Cybersecurity implications – vulnerability to hackers
   4.3. Cybersecurity implications – vulnerability to ‘false warrants’

1. SUMMARY OF FUNCTION AND NEED FOR IPB

The IPB represents both a continuation of the push for more investigatory powers, as was the case with the “emergency” Data Retention and Investigatory Powers Act of 2014 (DRIP), as well as a response to the ‘Snowden revelations’ regarding numerous (mass) surveillance operations (e.g. Tempora) by GCHQ, which revealed a lack of judicial oversight and transparency in the procedures governing surveillance by UK national security agencies.

The need for a systematic review and overhaul of the regulations regarding intelligence gathering, especially from the internet, certainly exists. At present the UK regulations on this are a patchwork of, often rushed, regulations including:

- Data Retention and Investigatory Powers Act of 2014 (DRIP)
- Police Act 1997
- Justice and Security act 2013 (JSA)
- Intelligence Services act 1994
- Section 94 of the Telecommunications Act

With the results that oversight regarding the use of surveillance by UK security agencies is split between:

- Parliamentary oversight carried out by the cross-party ISC
The Interception of Communications Commissioner (IoCC) who oversees how public authorities use their interception and communications data powers under RIPA and powers under section 94 of the Telecommunications Act.

The Chief Surveillance Commissioner (CSC) who oversees how law enforcement agencies use covert surveillance powers and covert human intelligence sources under RIPA Part II and the Police Act 1997.

The Intelligence Services Commissioner (ISCom) who oversees how the intelligence agencies use the powers available to them under RIPA Part II (covert surveillance and covert human intelligence sources) and the Intelligence Services Act 1994.

Investigatory Powers Tribunal (IPT) which investigates complaints that law enforcement and the security and intelligence agencies have used their covert investigative techniques unlawfully or claims that the intelligence or law enforcement agencies have breached human rights legislation. It is an independent Tribunal comprised of judges and senior members of the legal profession.

As a result, even civil rights organizations like Open Rights Group (ORG) have for some time now been calling for a revision of the complete surveillance regulation.

The new bill provides a framework of warrants for the security and intelligence agencies to engaging in:

- Interception and examination of communications data
- Obtaining of communications data (a.k.a. meta-data)
- Require Communications Service Providers (i.e. any company that has anything to do with communications data, including ISPs, social network providers (e.g. Facebook), hardware manufacturers (e.g. Cisco) etc.) to retain communications data
- Engage in equipment interference (i.e. computer/device hacking)
- Bulk data interception (i.e. untargeted mass collection of data)
- Bulk data acquisition
- Bulk equipment interference

The warrant will be issued by the Secretary of State and must be approved by a Judicial Commissioner before coming into force (except in the case of ‘exceptional circumstances’ in which case the warrant must be approved by a Judicial Commissioner within five days). Grounds on which warrants can be applied for are:

1. The interest of national security
2. Preventing or detecting serious crime
3. In response to a request from a foreign agency with which there exists an international mutual assistance agreement
4. Safeguarding the economic well-being of the UK (in circumstances relevant to the interests of national security)

In each case, the warrant must be specific, detailing the kind of investigation that will be undertaken and its duration, which must be “necessary and proportionate to what is sought to be achieved”.

Unfortunately my reading of the IPB has failed to provide any clear definitions for what constitutes ‘interest of national security’, the definition of ‘serious crime’ or a clear concept of ‘necessary and proportionate’ (for Interception of communications, i.e. content of messages, there is a clause requiring that there must be sufficient indicating that the sought information could not reasonably be obtained by other means). For each of these it seems we would have to trust in the judgement of the Secretary of State and the Judicial Commissioner. Before taking a closer look at the proposed
position of Judicial Commissioner. I should also point out that recent history, revealed by Snowden documents, suggests that 3. will need to be closely monitored to prevent it being abused by close collaboration between agencies for circumventing national restrictions (e.g. if NSA putting in a request of behalf of GCHQ). Also, it is not at all clear to me why 4. is included as a possible ground for applying for a warrant. If “safeguarding the economic well-being of the UK” is being pursued “in circumstances relevant to the interest of national security”, couldn’t the warrant be applied for under the ground of “interest of national security”, i.e. 1.? The inclusion of 4. thus has a strong sense of ‘industrial espionage’ to it.

It should also be noted that an additional ground (not mentioned in the summary of the bill) for which warrants can be given is for “testing or training activities”, defined as:

a) the testing, maintenance or development of apparatus, systems or other capabilities relating to the interception of communications in the course of their transmission by means of a telecommunication system or to the obtaining of related communications data, or

b) the training of persons who carry out, or are likely to carry out, such interception or the obtaining of such data.

Such ‘testing or training’ warrants clearly present another potential for abuse of power unless they are very closely monitored.

2. MANDATE OF PROPOSED JUDICIAL OVERSIGHT

One of the much vaunted features of the IPB by the Home Secretary is the so called ‘double lock’ provided by the requirement that the Judicial Commissioner has to sign off on any warrant in order for it to take effect. So what do we know about the position of the Judicial Commissioner, and how they will be appointed?

“The draft Bill will create a single new independent and more powerful IPC [Investigatory Powers Commissioner]. The Commissioner will be properly supported and will have a significantly expanded role in authorising the use of investigatory powers and a wide-ranging and self-determined remit to oversee any aspect of how law enforcement and the security and intelligence agencies use the powers and capabilities available to them.

The IPC will be a senior judge and with his supporting staff will have three key roles:

1. To authorise and approve the use of investigatory powers. Judicial Commissioners, who will be serving or former High Court judges, will undertake this role.

2. There will be an inspection role. The IPC will audit compliance and undertake investigations. Judicial Commissioners will undertake this role and will be supported by a team of expert inspectors.

3. The new Commissioner will have a clear mandate to inform Parliament and the public about the need for and use of investigatory powers. The Commissioner will report publicly and make recommendations on what he finds in the course of his work. He will also publish guidance when it is required on the proper use of investigatory powers. The Commissioner will have a strong public profile and active media and online presence so that he is quickly established as an authoritative source of advice and information. To support these three roles, the Commissioner will also have dedicated legal, technical and communications support.”

While the mandate of the Commissioner to inform Parliament and the public about the use of investigatory powers through an annual public report appears promising, the draft IPB unfortunately
provides no further indications about the level of detail that should be expected in such a report. It is therefore very likely that such a report would be restricted to the barest of statistic, especially since the security agencies are likely to cite ‘national security requirement’ as a reason for obscuring as much as possible about their activities.

3. CONCERNS REGARDING PROPOSED APPOINTMENT PROCEDURE FOR JUDICIAL OVERSIGHT

On the topic of how the IPC and Judicial Commissioners are to be appointed, the draft IPB states:

1) The Prime Minister must appoint—
   a) the Investigatory Powers Commissioner, and
   b) such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the functions of the Judicial Commissioners.

2) A person is not to be appointed as the Investigatory Powers Commissioner or another Judicial Commissioner unless the person holds or has held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005).

3) Before appointing any person under subsection (1), the Prime Minister must consult—
   a) the Scottish Ministers, and
   b) the First Minister and deputy First Minister in Northern Ireland.

4) Before appointing a Judicial Commissioner under subsection (1)(b), the Prime Minister must also consult the Investigatory Powers Commissioner.

5) The Prime Minister must inform the Scottish Ministers and the First Minister and deputy First Minister in Northern Ireland of an appointment under subsection (1).

6) The Investigatory Powers Commissioner is a Judicial Commissioner and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners.

Clearly, with the exception of a rather vague requirement to ‘consult’ with the Scottish Ministers and the First Minister and deputy First Minister in Northern Ireland, the appointment of these vital Commissioners, who must provide the independent oversight on the decisions of the Secretary of State, is completely in the hands on the Prime Minister. Nowhere is there any requirement for parliamentary approval or public scrutiny.

4. KEY AREAS OF CONCERN EXPRESSED BY INDUSTRY AND CIVIL RIGHTS ORGANIZATIONS

Two clauses, which apply to each of the types of warrants (Interception and examination of communications data; Obtaining of communications data; Require Communications Service Providers to retain communications data; Engage in equipment interference; Bulk data interception; Bulk data acquisition; Bulk equipment interference) and which have cause most of the concern from industry as well as civil rights organisations, are the “Duty of operators to assist with implementation” and the “Duty not to make unauthorised disclosures”.

4.1 Implications for customer trust and independent monitoring by journalists/civil rights groups

The “Duty of operators to assist with implementation” means a Communications Service Providers (CSP), or even private individuals, would be required to do everything that is reasonably doable to help the security services in collecting data, decrypting communications (via deliberate security
weaknesses, i.e. ‘backdoors’) and hacking into systems/service they the CSP provides to its customers. The “Duty not to make unauthorised disclosures” means that it would be a criminal offense for the CSP to notify anyone of the fact that they had been compelled to cooperate with such a warrant. This would seriously undermine the ability of CSPs to engender trust in any of their security product, e.g. Apple’s end-to-end encrypted iMessenger. The fact that companies would not even be allowed to provide statistics about the number of warrants they had been served would also dramatically reduce the ability for journalists and civil rights organisations to independently monitor the level of state surveillance.

4.2 Cybersecurity implications – vulnerability to hackers

There is also a great deal of concern regarding the implications for cybersecurity. On the one hand, it has been shown that backdoors to unlocking encrypted services fundamentally undermine overall security, or as Apple phrased it in their comments to the draft IPB: “A key left under the doormat would not just be there for the good guys. The bad guys would find it too.” On the other hand, potentially requiring CSPs to retain large amounts of meta-data for up to 12 months could produce very attractive targets for cybercriminals who are interested in any information about people’s online behaviours in order to ‘optimize’ attacks such as phishing.

4.3 Cybersecurity implications – vulnerability to ‘false warrants’

A third potential cybersecurity vulnerability, that has not been discussed much, is the potential criminals to con people into believing that they were being served a genuine ‘equipment interference’ warrant, especially since the “duty not to make unauthorised disclosures” might stop them from being able to adequately verify any such warrant.

January 2016