Written Evidence from Institute for Human Rights and Business (IHRB) (DIP00012)

Summary

The Institute for Human Rights and Business (IHRB) welcomes the opportunity to submit written evidence to this inquiry. IHRB has already submitted comments and recommendations to the Science and Technology Committee focused on the impact on communications service providers and related businesses and the likely consequences for citizen/consumer use of ICT services arising from the technology aspects in the draft Investigatory Powers Bill (the draft Bill). Here, we focus on any significant human rights issues raised or likely to be raised by the draft Bill, and what more could be done to enhance the protection of human rights, as requested by the Joint Committee on Human Rights.

The comments provided in this submission are concerned mainly with the right to privacy and draw on IHRB’s previous research developing a “Rights Respecting Model for Communications Surveillance through Lawful Interception and Government Access to User Data” (see here, p.35). This model sets out important principles for each step of developing and implementing a communications surveillance legal framework that protects and respects human rights, and will shortly be published as an IHRB Occasional Paper. Our comments also draw on recent reports to the UN General Assembly and Human Rights Council.1 The main points concern:

1. The Right to Privacy
2. Bulk Collection of Data
3. Internet Connection Records
4. Data Retention
5. Judicial Authorisation of Warrants
6. Oversight
7. Access to Remedy

---

1 These recommendations draw on recent reports to the UN General Assembly and Human Rights Council, including the Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/23/40 (June 2013); The Right To Privacy in the Digital Age, UN Resolution 68/167 adopted 21st January 2014; Report of the Office of the United Nations High Commissioner for Human Rights, presented to the Human Rights Council in September 2014 A/HRC/27/37 and the Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism to the UN General Assembly in September 2014 A/69/397
1. The Right to Privacy

1.1 In this age of widespread digital communications, the realisation of human rights, including the right to privacy, entails a complex balancing act between the obligations of governments to protect those rights, the responsibilities of companies that provide communications services to respect those rights and the ability of users of those services to enjoy those rights. It can be argued that there is no respect for human rights in the absence of a secure society, and no security without respect for human rights. Governments have a duty to protect citizens from terrorism and other threats and therefore can have legitimate reasons to initiate surveillance of a person’s communications. But they must address the demands for security within the context of protecting other fundamental freedoms. Intercepting or monitoring communications is an intrusive process for individual privacy and therefore any such actions should be governed by a strict legal framework to prevent arbitrary violations of privacy and freedom of expression.

1.2 Under human rights law, the right to privacy is a qualified human right; governments can legitimately restrict the right and intrude on people’s privacy provided a number of specific conditions are met.

1.3 Under Article 17 of the International Covenant on Civil and Political Rights (ICCPR), any restrictions on the right to privacy must not be either unlawful or arbitrary. In the recent report, “The Right to Privacy in the Digital Age,” presented to the UN Human Rights Council in June 2014, the UN High Commissioner for Human Rights explains these restrictions further:

(i) “Unlawful”: A restriction is “unlawful” when it is not authorised by States on the basis of national law specifically authorising interference. The national law must be sufficiently accessible, clear and precise and also must not conflict with other provisions of the ICCPR, such as the prohibition on discrimination or the country’s own constitution or

(ii) “Arbitrary”. The protection against “arbitrary interference” means that the interference should be reasonable in the particular circumstances. It must be in proportion to the aim and the least intrusive option available to accomplish the aim and be necessary in the circumstances for reaching a legitimate aim.

1.4 The same report highlights that the onus is on the relevant authorities to show that proposed limitations on the right to privacy are connected with a legitimate aim. The limitation must also be shown to have some chance of achieving that goal while at the same time not being so overly restrictive that the restriction makes the exercise of the right meaningless. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.

1.5 With this in mind, we ask the Committee to particularly scrutinise the bulk collection of data powers and the collection and retention of Internet Connection Records (ICRs) in the draft Bill.

---

2 See UN Resolution 68/167 The Right to Privacy in the Digital Age (21 January 2014), which affirms that the same rights that people have offline must also be protected online.
4 Ibid, para 23.
2. Bulk Collection of Data

2.1 Publicly avowed for the first time in the draft Bill are many bulk collection capabilities, which civil society groups have subsequently challenged, in and out of UK and European courts. In the draft Bill there are provisions for *bulk interception of communications*, *bulk collection of communications data*, the acquisition and use of *bulk personal datasets* and provisions for *bulk equipment interference*.

2.2 Bulk collection of data is authorised by thematic/class based warrants - these warrants do not name individuals or addresses but rely on generalised categories of people or places. This means that the communications of potentially millions of people not suspected of any crime will be collected and stored. This is acknowledged in the draft Bill; for example in the *Draft Investigatory Powers Bill: Guide to Powers and Safeguards*, Bulk Personal Datasets are described as, “sets of personal information about a large number of individuals, the majority of whom will not be of any interest to the security and intelligence agencies.”

2.3 Communications surveillance must be limited to that necessary to achieve a legitimate aim and use the means least likely to infringe rights – it must be both necessary and proportionate. An objective assessment of the necessity and proportionality of the contemplated surveillance is stated as a core part of the authorisation process in the draft Bill. However, the broad use of bulk powers and thematic/class based warrants which are likely to collect personal information of individuals not suspected of any crime, makes the necessary and proportionate test extremely difficult, if not impossible to conduct.

2.4 UN experts have indicated serious concern about communications surveillance that is authorised on such a broad and indiscriminate basis. Actions of this scope are seen as running counter to the whole core concept of the protection of privacy that requires justification for intrusions on privacy to be made on a case-by-case basis.\(^5\)

2.5 The Committee should robustly question the safeguards currently outlined in the draft Bill, and the criteria under which bulk collection of data would be considered necessary and proportionate.

3. Internet Connection Records (ICRs)

3.1 The Home Secretary has described ICRs as the “equivalent of an itemised phone bill”. In the case of resolving an IP address (finding out who used a particular service), this would show, for example, that a particular smartphone was connected to a particular email service at a particular time. However, ICRs also reveal websites visited (but not the individual page). This is not the equivalent of an itemised phone bill, and the collection and use of ICRs requires further scrutiny.

3.2 Knowing a user has visited a general purpose website like www.google.com doesn’t reveal much about an individual. Knowing a user has visited more specific sites such as www.lgbt.foundation does however. In addition, under the draft Bill neither the police or intelligence and security services would need a warrant to obtain this information. In certain cases it may be needed to access this kind of ICRs (for example if someone was accessing an illegal website), but it does not seem accurate to describe these as the equivalent of an itemised phone bill, as the Home Secretary suggested and as there is no authorisation

required in the draft Bill, the necessary and proportionate test has been removed to justify the privacy intrusion.

3.3 The Committee should examine further whether ICRs would be considered content, and therefore should be subject to stronger legal protections under the draft Bill.

4. Judicial Authorisation

4.1 The draft Bill provides a “double lock” on authorisation of warrants for certain interception and acquisition of data: A warrant is signed by the Secretary of State and a member of the Judiciary. However, on closer inspection of the draft Bill, it appears the judiciary’s main role is checking whether the Secretary of State has followed correct procedures in authorising the warrant, rather than rendering a judgment on the evidence presented to authorise the warrant. In addition, in “urgent” cases, the Secretary of State can authorise a warrant without judicial approval. In these cases, the judge can only give approval retrospectively.

4.2 The Committee should analyse the role of the judiciary in authorising warrants, to ensure there is a meaningful “double-lock” on approving warrants.

5. Data Retention and Storage

5.1 In April 2014, the European Court of Justice (ECJ) declared the EU Data Retention Directive invalid, due to “wide ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary.”

5.2 To replace the powers in the EU Data Retention Directive, the UK government then enacted the Data Retention Investigatory Powers Act (DRIPA 2014), which is due to expire at the end of 2016. The draft Bill creates a new statutory basis for retention of communications data. ICRs can be stored for up to 12 months, and warrants for bulk powers such as equipment interference, interception, and acquisition of data can last for up to 6 months, with seemingly unlimited options for renewal.

5.3 Companies required to retain their customer ICRs for twelve months will be served with a Data Retention Notice issued by the Secretary of State, when it is deemed “necessary and proportionate” to do so. It is unclear which companies can expect to receive such notices and the conditions under which it would be necessary and proportionate to retain all user ICRs.

5.4 Transparency is extremely important in order to build trust among stakeholders. Companies should be able to be transparent with users about the collection, storage and access of ICRs and should not be prevented from including any requests for datasets in their transparency reports.

5.5 The Committee should examine whether the data retention proposed in the draft Bill is in line with international standards, taking into account the ECJ judgment.

6. Oversight

6.1 The draft Bill replaces three existing oversight bodies - the Interception of Communications Commissioner (IOCC), the Chief Surveillance Commissioner (CSC) and the Intelligence Services Commissioner (ISCom) - with one Investigatory Powers Commissioner (IPC), who will be a senior judge with supporting staff.

6.2 The IPC must have access to all potentially relevant information to enable it to evaluate whether the state is carrying out its activities in a lawful way. This must include secret and classified information. This is to ensure oversight is rigorous and not a “rubber stamping” exercise.

6.3 Consideration should be given to permitting a confidential public interest advocate, for example an independent human rights expert, to be part of the IPC’s staff to ensure that appropriate consideration is given to the human rights implications of requests. This is particularly important given the high degree of secrecy of authorisation processes that relate to national security.

6.4 Third parties, including companies, should have the ability to bring information to the IPC where relevant.

6.5 Where a violation is identified, the IPC must be able to order the termination of the surveillance and the deletion of data and the prohibition of its use by issuing binding orders.

7. Access to Remedy

7.1 In cases where surveillance powers are misused, either intentionally or otherwise, there should be redress and remedy. But individuals need to know whether they have been subject to surveillance in order to bring a complaint to the Investigatory Powers Tribunal (IPT) and seek access to remedy.

7.2 It is understood that there will be times when individuals cannot be notified that they are under surveillance as doing so could jeopardise the surveillance itself. However, notifying individuals if they have been the subjects of surveillance is an important element of access to remedy for those who may have been subject to illegal surveillance. At a minimum, users should be notified that their communications have been subject to surveillance when the surveillance is complete. Such a provision is absent from the draft Bill.

7.3 The legal framework should set out the circumstances under which there may be a delay in individuals being notified that they are under surveillance. When individuals are informed that they have been the subjects of surveillance they should also be informed of the procedure for filing a complaint with the IPT if they wish to do so.

*****

About IHRB
IHRB is a global centre of excellence and expertise on the relationship between business and internationally recognised human rights standards.

We work to shape policy, advance practice and strengthen accountability to ensure the activities of companies do not contribute to human rights abuses, and in fact lead to positive outcomes.

IHRB prioritises its work through time-bound programmes that can have the greatest impact, leverage and catalytic effect focusing on countries in economic and political transition, as well as business sectors that underpin others in relation to the flows of information, finance, workers and/or commodities.

December 2015