Written evidence submitted by
The Institute for Human Rights and Business (IHRB) (IPB0035)

SUMMARY

The Institute for Human Rights and Business (IHRB) welcomes the opportunity to submit written evidence to this inquiry. A particular focus of IHRB’s work with respect to the Information and Communications Technology (ICT) sector has been on how government surveillance powers may adversely impact the ability of ICT companies to effectively implement their responsibility to respect human rights as set out in the UN Guiding Principles on Business and Human Rights. IHRB will provide additional comments to the Joint Committee on Human Rights in this regard.

This submission provides comments and recommendations 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) as requested by the Science and Technology Committee. The main points concern:

1. **The draft Bill’s definition of telecommunication services and systems**: Companies outside of the ICT sector are developing products and services relying on the collection of data and use of communications services, and therefore should be included in forthcoming consultations.

2. **Bulk Personal Datasets**: Provisions in the draft Bill allow access to bulk personal datasets, which will increase in volume due to the advent of the “Internet of things” and “big data” thus raising important questions with respect to surveillance.

3. **Obligations on overseas companies**: The draft Bill also applies to overseas companies, but it is unclear how these obligations will be enforced.

4. **Encryption**: It is likely the draft Bill will not eliminate end-to-end encryption, but it will prevent companies served with a technical capability notice from offering end-to-end encryption as part of their services. This will have an impact on the security of many services relied upon every day by millions of users, such as online banking, and secure communications relied on by those in sensitive professions such as lawyers, doctors and journalists.

5. **Internet Connection Records (ICRs) and Data Retention Notices**: As this is a new provision in the draft Bill, it will require particular scrutiny. There are questions as to how collecting and storing ICRs is technically possible, and whether Data Retention Notices to retain all user ICRs are “necessary and proportionate”. In addition, there are questions as to how transparent companies can be with their users about the collection and storage of ICRs.

6. **Cost of implementation**: While the costs of developing new or configuring existing systems may be high, it is important that any Government promise of compensation to companies does not become an economic incentive or additional funding stream for companies, or serve in any way as a disincentive for companies to uphold the corporate responsibility to respect human rights.

1. **DEFINITION OF TELECOMMUNICATIONS SERVICES AND SYSTEMS**

1.1 In Section 193 (Telecommunications Definitions) of the draft Bill, telecommunications services and systems are defined as:

(11) “Telecommunications service” means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service).

(12) For the purposes of subsection (11), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system.
“Telecommunication system” means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.

1.2 With the development of the “Internet of things” and “big data”, in the near future this definition could encompass a much wider range of companies that rely on Internet services to deliver products and services. The issue of surveillance is no longer confined to the ICT sector and is likely to become a cross-sector issue that impacts a wider range of companies.

1.3 It is unclear whether the current definition includes devices that generate data relating to individuals that may not involve communication between two people, but instead machine-to-machine communication. For example, automated infrastructure involved in the collection of data relating to cars, wearables (such as fitness) or energy smart meters. Could the Committee envisage situations in which companies generating datasets relating to geo-location (such as Internet-connected cars) or energy use (such as gas/electric smart meters) would be served with a data retention notice?

1.4 The public debate around the draft Bill has largely focused on user-facing communication services such as mobile services, messaging applications and search and the resulting impact on privacy. The debate has not yet touched on other data generating services that may fall under this draft Bill, and the resulting impact on user privacy.

Recommendation:

- The Committee should consider whether the definition of telecommunications services could result in companies outside of the ICT sector receiving a technical capability notice under Section 189 (Maintenance of technical capability).
- The Committee should consider including companies outside of the ICT Sector in forthcoming consultations in order to further understand how the draft Bill could impact these companies e.g. the automobile industry and energy sector.

2. Bulk Personal Datasets

2.1 If the definition of telecommunication services is as broad as outlined in Section 1 above, Bulk personal datasets in the near future could encompass a wide range of information held by a wide range of companies.

2.2 In a separate inquiry by the Science and Technology Committee on The Big Data Dilemma, the Committee has received written evidence outlining the importance of Big Data to the UK economy. For example, techUK outlined the importance of Big Data analytics to the UK economy, both in terms of GDP and employment and also increasing productivity, in their written evidence submitted in September 2015. The Centre for Economic and Business Research estimated that by 2017 Big Data could contribute £216 billion and generate 58,000 new jobs in the UK and Ireland.

2.3 Big data and surveillance are linked, as the collection and storage of large datasets for one purpose could be accessed by security and intelligence agencies as outlined in the provision for bulk personal datasets. In the guide Assessing Cybersecurity Export Risks (produced by HM Government, techUK and IHRB), “Analytics and Big Data” was flagged as a capability that had a potentially negative impact on human rights including privacy. The guide provided the example that,

“In principle, the correlation of different data sets can (re)identify an individual and provide information about them that is even more private than the data they consented to share, such as their religion, ethnicity and sexual orientation. This can be achieved by combining data from closed and open sources.” (P15)
2.4 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.”

2.5 Therefore, with so much personal data potentially accessed by security services, there is a question as to whether users are aware of what kind of personal information is being collected and stored by various organisations, which may end up being accessed by the security services. In turn, if companies are obliged to hand over their bulk datasets to security services but are prevented from disclosing this fact, this could damage user trust in companies.

Recommendation:

• The Committee should apply learning from the Big Data Dilemma inquiry, in particular regarding explicit user informed consent and data security.

3. OVERSEAS COMPANIES

3.1 The draft Bill states that it “places the same obligations on all companies providing services to the UK or in control of communications systems in the UK.”

Companies based overseas would therefore fall under the draft Bill, but it is not clear how relevant obligations will be enforced. On the publication of the draft Bill, Yahoo! published a blog outlining initial concerns about how the UK government would affirm extraterritorial jurisdiction on overseas service providers: “National laws cannot solve an international problem. If emulated around the world, the UK Government’s extraterritoriality clause would create a chaotic legal environment and unpredictability for companies, users, and agencies.”

Representatives from the ICT sector presenting oral evidence to the Science and Technology Committee session on 10 November 2015 expressed concern at the impression that UK-based companies were under a greater obligation to disclose data, putting them at a commercial disadvantage over non-UK based companies. This in turn would also impact UK companies’ responsibility to respect human rights, such as privacy.

3.2 Debates relating to the extraterritorial nature of data and access continue as can be seen, for example, in the case Microsoft vs. Ireland. The Independent Reviewer of Terrorism Legislation, David Anderson, looked at the issue of international data sharing in his June 2015 report, A Question of Trust and concluded, “there is no immediate solution in sight” (11.28).

3.3 The Prime Minister’s Special Envoy on Intelligence and Law Enforcement Data Sharing, Sir Nigel Sheinwald, put forward proposals in a June 2015 briefing to strengthen Government to Government co-operation, reforming the Mutual Legal Assistance Treaty (MLAT) (which has been supported by many overseas companies) and building a new international framework for data sharing.

Recommendations:

• The Committee should consider making inquiries as to how the draft Bill, in the current climate of uncertainty over international data sharing, will be enforced on overseas companies.
• The Committee should consider inviting overseas companies (from the USA and other regions) to give written and oral evidence at forthcoming consultations.
• The Committee should investigate how to speed up or implement Sir Nigel Sheinwald’s recommendations on building a new international framework for data sharing.

4. ENCRYPTION
4.1 In the build up to the publication of the draft Bill, there was much speculation that the Government would ban encryption, or insist on communication “backdoors” which would put everyone’s digital security at risk, impact the right to privacy and potentially result in a “chilling effect” on freedom of expression. While it appears the Government supports encryption to a certain extent, the obligations placed on companies in the Bill are unclear in this regard. Under Section 189 (Maintenance of technical capability), “relevant operators” have, 4(c) obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data;

4.2 This is widely believed to refer to end-to-end encryption, where no actor holds the “keys” to decrypt communications and are therefore impossible to intercept. If so, companies offering telecommunication services which are served with a technical capability notice will have to comply, which essentially means that only these companies are unable to offer end to end encryption to their customers. It is therefore likely that end-to-end encryption will not cease to exist, but the draft Bill will essentially prevent large telecommunication companies from offering end-to-end encryption on their services, which will have a significant impact on the security of products and therefore viewed by users as less secure than others.

Recommendations:

• The Committee should seek to clarify the obligations placed on companies in Section 189 4(c).
• The Committee should assess the impact on users that rely on end-to-end encryption for both commercial and personal security, such as banks, lawyers and journalists if telecommunication services companies served with a technical capability notice are unable to offer end-to-end encryption.

5. INTERNET CONNECTION RECORDS (ICRs) AND DATA RETENTION NOTICES

5.1 As this is a new provision in the Bill, it will require particular scrutiny. IHRB will address the impacts on privacy of retaining ICRs further in separate consultation, but there are questions as to how collecting and storing ICRs is technically possible. During a recent session of the Science and Technology Committee, witnesses from the ICT Sector expressed concern about how the separation of content and communications data in this context could technically happen.

5.2 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 this and the conditions under which it would be necessary and proportionate to retain all user ICRs.

5.3 In addition, there is a question as to how telecommunication companies will communicate this complex act to their users. It is misleading to describe 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 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. Knowing a user has visited www.google.com doesn’t reveal much, but knowing a user has visited www.lgbt.foundation does. In addition, 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, and as there is no authorisation required, the necessary and proportionate test has been removed.

Recommendations:

• The Committee should particularly scrutinise how the collection and storage of ICRs will be carried out from a technical perspective.
6. PAYMENTS TOWARDS COMPLIANCE COSTS

6.1 Section 185 provides arrangements for telecommunications operators receiving “an appropriate contribution in respect of relevant costs.” Relevant costs “means costs incurred, or likely to be incurred, by telecommunications operators and postal operators in complying with this Act.”

Companies may have to develop new, or configure existing systems to collect data required under various technical capability notices, and increase storage capacity which will incur significant costs. In initial comments, the Internet Service Providers Association (ISPA) raised concerns,

“Despite provisions around ISPs’ costs potentially being covered by the Government, compliance procedures may hamper innovation and distract businesses from concentrating on their key services.”

Recommendation:

- It is important to ensure that any promises of compensation do not become an economic incentive or additional funding stream for companies, and should not serve as a disincentive to uphold the corporate responsibility to respect human rights.

ABOUT IHRB

IHRB is a global centre of excellence and expertise (a think & do tank) 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.

November 2015