Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc., Yahoo Inc.—written evidence (IPB0116)

INTRODUCTION

1. National security is an important concern for Governments. Governments have a responsibility to protect people and their privacy. We believe a legal framework can protect both. Our companies want to help establish a framework for lawful requests for data that, consistent with principles of necessity and proportionality, protects the rights of the individual and supports legitimate investigations.
2. As members of the Reform Government Surveillance (RGS) coalition (www.reformgovernmentsurveillance.com), we believe the best way for countries to promote the security and privacy interests of their citizens, while also respecting the sovereignty of other nations, is to ensure that surveillance is targeted, lawful, proportionate, necessary, jurisdictionally bounded, and transparent. These principles reflect the perspective of global companies that offer borderless technologies to billions of people around the globe.
3. The actions the UK Government takes here could have far reaching implications – for our customers, for your own citizens, and for the future of the global technology industry. While we recognize the UK Government has made efforts to develop a clear, comprehensive and modern legal framework, we would offer several important considerations that shape our view of the Bill:
    - User trust is essential to our ability to continue to innovate and offer our customers products and services, which empower them to achieve more in their personal and professional lives.
    - Governments' surveillance authorities, even when transparent and enshrined in law, can undermine users' trust in the security of our products and services.
    - Key elements of whatever legislation is passed by the UK are likely to be replicated by other countries, including with respect to UK citizens' data.
    - Unilateral imposition of obligations on overseas providers will conflict with legal obligations such providers are subject to in other countries.
    - An increasingly chaotic international legal system will leave companies in the impossible position of deciding whose laws to violate and could fuel data localization efforts.
4. We appreciate the opportunity to consult on the Bill. To that end, we advance a number of issues that we believe are important to serve UK citizens and the citizens of other nations, while ensuring that citizens' human rights and privacy rights are protected. This includes ensuring the Bill satisfies ECJ scrutiny and also builds greater legal certainty and consistency for the proposed measures.

PRIMARY CONCERNS

1. **Extraterritorial Jurisdiction (ETJ)**
    a) **Conflict of laws:** As noted earlier, we anticipate that other countries will emulate what the UK does here. Unilateral assertions of extraterritorial jurisdiction will create conflicting legal obligations for overseas providers who are subject to legal obligations elsewhere. The UK Government understood this in 2009, when the Home Office Consultation 'Protecting the Public in a Changing Communications Environment' stated that RIPA did not apply to overseas providers. Conflicts of laws create an increasingly chaotic legal environment for providers,

restricting the free flow of information and leaving private companies to decide whose laws to violate. These decisions should be made by Governments, grounded in fundamental rights of privacy, freedom of expression, and other human rights.

If the UK legislation retains authority to reach extraterritorially, the Bill should consistently and explicitly state that no company is required to comply with any notice/warrant, which in doing so would contravene its legal obligations in other jurisdictions. Enforcement obligations should also take this into account. Notwithstanding our position, currently there is confusion: the context section of the Bill overview document states, "Enforcement of obligations against overseas CSPs will be limited to interception and targeted CD acquisition powers". This is not what the Bill itself says.

b) **International framework:** We agree with the recommendation of Sir Nigel Sheinwald and others that an international framework should be developed to establish a common set of rules to resolve these conflicts across jurisdictions. These rules should facilitate more efficient requests in cases that provide adequate protections for user privacy. There are indications in the legislation that the UK Government has identified an approach that could work. Though interception is generally prohibited, for example, the Bill permits interception in the UK when it is done "in response to a request made in accordance with a relevant international agreement." If the UK Government's authority should have unlimited application overseas, it is unclear why the UK Government believes other countries' authorities should only extend into the UK pursuant to an international agreement. Instead, a better approach would be to condition the extraterritorial application of UK law to situations where it is done pursuant to an international agreement that permits it, and furthermore resolves conflicting obligations in the other country.

c) **Service of warrants on overseas providers:** The Bill permits warrants to be served on companies outside the UK in a number of ways, including serving it on principal offices within the UK. Despite ETJ language, this presents a risk to UK employees of our companies. We have collective experience around the world of personnel who have nothing to do with the data sought being arrested or intimidated in an attempt to force a overseas corporation to disclose user information. We do not believe that the UK wants to legitimize this lawless and heavy-handed practice.

2. **Technical impositions:**

a) **Clarity on encryption:** The companies believe that encryption is a fundamental security tool, important to the security of the digital economy as well as crucial to ensuring the safety of web users worldwide. We reject any proposals that would require companies to deliberately weaken the security of their products via backdoors, forced decryption, or any other means. We therefore have concerns that the Bill includes *"obligations relating to the removal of electronic protection applied by a relevant operator to any communication or data"* and that these are explicitly intended to apply extraterritorially with limited protections for overseas providers. We appreciate the statements in the Bill and by the Home Secretary that the Bill is not intended to weaken the use of encryption, and suggest that the Bill expressly state that nothing in the Bill should be construed to require a company to weaken or defeat its security measures.

b) **No business should be compelled to generate and retain data that it does not ordinarily generate in the course of its business**. Some language under the retention part of the Bill suggests that a company could be required to generate data – and perhaps even reconfigure their networks or services to generate data – for the purposes of retention.

3. Judicial authorization:

a) **Judicial review standard:** As recommended by David Anderson QC, Governments should not be able to compel the production of private communications content absent authorization from an independent and impartial judicial official. While we believe the Bill's 'double lock' represents an important step in the right direction, there remains room for improvement. The "judicial review" standard should be clarified to ensure that the judge reviews the actual merits of the matter, and not just the process by which decisions and actions were taken by the authorizing secretary. To truly serve as a second lock, this function must not just assess the rationality or reasonableness of the ministerial decision, but ensure that investigatory warrants under the Bill will withstand the full scrutiny of a court.

b) **Applicability:** we believe that judicial authorization should be applied to a broader set of authorities and also be extended to national security notices, maintenance of technical capability orders, and modifications to equipment interference warrants which have been issued to the Chief of Defence Intelligence and intelligence services.

4. **Bulk collection**

a) **Explicit language:** As set forth in the Reform Government Surveillance principles, surveillance laws should not permit bulk collection of information. The principles require that the Government specifically identify the individuals or accounts to be targeted and should expressly prohibit bulk surveillance. The word "bulk" can be ambiguous. We understand from David Anderson QC's report that, in the UK, bulk warrants allow a specific communications channel external to the UK to be specified due to the link with a specific national security or serious crime threat. It is then filtered and searched for identifiers. In terms of setting international precedent, we therefore suggest that the Bill be more explicit in the language it uses, highlighting that any collection should be pursuant to a specific identifier.

b) **Minimization provisions:** We also believe that the general safeguards sections should explicitly include 'minimization' provisions, ensuring that only the necessary and proportionate amount of data is obtained, analyzed and retained. All other data should be destroyed.

5. **Transparency and Clarity**

a) **Elimination of Vague and Confusing Language:** As David Anderson QC highlighted in '*A Question of Trust*', legislation on surveillance powers should be written in such a way that the intelligent reader can understand the surveillance powers possessed by the Government, and how, where and by whom they are used. Legislation or practice that is wide-reaching and vague harms the ability of the users and companies to understand government surveillance. It also impacts on the ability of formal and informal oversight mechanisms, including NGOs, to carry out their function effectively. There are many aspects of the Bill which we believe remain opaque: judicial authorization; the extent of the obligations on companies outside of the UK; the confusing messages about the extent to which there is an obligation to produce material that can be read versus the Government's statement about the Bill not prohibiting encryption; and the obligations on technical capability. We outline additional suggestions in the document. We urge the Joint Committee and the Home Office to do all that it can to ensure that the whole Bill is written clearly and unambiguously.

b) **User notification:** As a general rule, users should be informed when the Government seeks access to account data. It is important both in terms of transparency, as well as affording users the right to protect their own legal rights. Our users range from individual consumers to large media organizations to large public sector entities. Even where the Government establishes a need to obtain certain information, it does not necessarily deprive users of other rights they may

have, and knowledge of the request is essential to their ability to advance those rights. While it may be appropriate to withhold or delay notice in exceptional cases, in those cases the burden should be on the Government to demonstrate that there is an overriding need to protect public safety or preserve the integrity of a criminal investigation.

c) **Warrant recipient:** We welcome the Bill's clarification that warrants must be both "necessary and proportionate." However, once there is a determination that a warrant is necessary, the question should then be to whom the warrant should be directed. It is our view that the same standard – "necessary" – should be applied when evaluating this question. In many cases, the Government can (and often does) obtain the information directly from the users themselves. When that is not possible, the Government should seek the information from the most proximate source with access to the data. An obvious example of this involves enterprise cloud customers. Even as private sector and public sector entities transition to the cloud, they remain in complete control of their own data. Before they moved data off of their own servers and onto the servers of large cloud providers, Governments would go to them for their data or the data of their employees. There is no reason Governments cannot continue to do the same after these organizations transition their data to the cloud. This is an area where the UK can lead the rest of the world, promoting cloud adoption, protecting law enforcement's investigative needs, and resolving jurisdictional challenges without acting extraterritorially.

d) **Overseas provider standing:** Overseas providers should have a legal right to seek legal advice and raise complaints with the Commissioner without either committing a disclosure offence or accepting jurisdiction. There should be the possibility for judicial commissioners to request amicus briefs from affected providers.

e) **Clarity on urgent provisions, e.g. approval of warrants issued in urgent cases**. The term "urgent" is not defined in the Bill. Clarity on this term - which other countries may seek to emulate and even abuse - is important.

6. **Computer Network Exploitation**:

a) **Risk to user trust:** The ultimate test we apply to each of the authorities in this Bill is whether they will promote and maintain the trust users place in our technology. Even where these authorities do not apply to overseas providers like our companies, we are concerned that some of the authorities contained in the Bill, as currently drafted, represent a step in the wrong direction. The clearest example is the authority to engage in computer network exploitation, or equipment interference. To the extent this could involve the introduction of risks or vulnerabilities into products or services, it would be a very dangerous precedent to set, and we would urge your Government to reconsider.

b) **Network integrity and cyber security requirements:** There are no statutory provisions relating to the importance of network integrity and cyber security, nor a requirement for agencies to inform companies of vulnerabilities that may be exploited by other actors. We urge the Government to make clear that actions taken under authorization do not introduce new risks or vulnerabilities for users or businesses, and that the goal of eliminating vulnerabilities is one shared by the UK Government. Without this, it would be impossible to see how these provisions could meet the proportionality test.

We are happy to follow up in writing with any queries you have on this written evidence, and undertake

to answer, via email, within 24 hours including during the holiday period. We are also happy to provide specific drafting comments, should you wish these.

Facebook Inc.

Google Inc.

Microsoft Corp.

Twitter Inc.

Yahoo Inc.

21 December 2015