Global Network Initiative (GNI)—written evidence (IPB0080)

1. The Global Network Initiative (GNI) welcomes the opportunity to provide this written submission to the Joint Committee on the Draft Investigatory Powers Bill. We have chosen to focus our submission on five specific issues, all of which relate to the United Kingdom's commitment to establish a world-leading legal framework and its important role as a standard setter for human rights and the rule of law around the globe:

   (I) Provisions on extra-territorial requests for user data
   (II) The need for a responsible and sustainable legal framework for international data
   (III) Authorisation of bulk collection of communications and communications-related data
   (IV) Provisions that would weaken encryption technologies
   (V) Absence of adequate mechanisms for transparency and accountability for surveillance powers

2. The GNI is a multi-stakeholder group of companies, civil society organisations (including human rights and press freedom groups), investors and academics, who have created a collaborative approach to protect and advance freedom of expression and privacy in the information communications and technology (ICT) sector. Formed in 2008, GNI has developed a set of Principles and Implementation Guidelines to guide responsible company action when facing requests from governments around the world that could impact the freedom of expression and privacy rights of users. These Principles and Implementation Guidelines are based on international human rights standards and are attached to this written evidence in Appendix A. Appendix B has a full list of participants and observers of GNI.

(I) Provisions on extra-territorial requests for user data

3. The GNI has previously expressed concern at provisions contained in the proposed Communications Data Bill of 2012 and the Data Retention and Investigatory Powers Act of 2014 which required communications service providers to respond to requests for user data relating to services operated outside of the U.K. government's jurisdiction.[1] The GNI notes that the Draft Investigatory Powers Bill would replicate and expand on these requirements by asserting jurisdiction over such services for seven out of the eight major powers contained in the Bill.[2]

4. By asserting extraterritorial jurisdiction, the draft Bill could provide unintended justification for similar actions by other governments, including those that seek to limit freedom of expression and other human rights online. We are concerned that the effect of passing this legislation will be to encourage other governments to expand claims of jurisdiction without regard to the law applicable to the service. We urge the Committee to be mindful of these consequences, including the risk of retaliatory action by other governments on the privacy rights of U.K. citizens at home and abroad, when considering this legislation. Extra-territorial assertions of jurisdiction create a conflict of laws situation and further complicate the international legal framework at a time when the goal for all stakeholders (users, government agencies and companies) is greater transparency and clearer accountability. This situation would increase uncertainty for all stakeholders and for the rights of U.K. and global citizens.

(II) The need for a responsible and sustainable legal framework for international data

5. The rise of global cloud computing, electronic payment platforms and social media, as well as a global security threat, makes urgent the creation of a responsible and sustainable international framework of laws for data. Independent reviews of the United Kingdom's investigatory and law enforcement data sharing powers performed by David Anderson QC, Sir Nigel Sheinwald, and the Royal United Services Institute delivered a broad consensus that the draft Bill must operate as part of a coherent international legal framework, which creates certainty for all stakeholders, clear laws on the acquisition of data, and sustainable solutions for the critical issues of jurisdiction and applicable law. The review performed by Sir Sheinwald in

particular recommended that the U.K. government make a concentrated effort to reform existing mutual legal assistance treaties (MLATs) and, where necessary, to develop new bilateral agreements for data. MLAT reform provides the best route to a sustainable and coherent legal framework, rather than the unilateral assertion of limitless jurisdiction as set out in the draft Bill.

6. The existing MLAT arrangements were designed as a mechanism for law enforcement to lawfully obtain data from other jurisdictions. They were negotiated by and between governments, with processes defined in a pre-Internet era. There has been limited modernisation in the intervening years and these processes, and the resources that support them, are today managing significantly higher demand and are under stress. GNI is particularly concerned that without significant reform to the MLAT system, governments around the world will increasingly act unilaterally through measures such as forced data localisation, government mandates that companies provide back doors into hardware or software, or demands that companies take steps that would compromise the security of users' communications.

7. We also note that strong independent judicial oversight is a crucial component in the international cooperation that will be needed to build a new international approach to data amongst democracies with a high respect for the rule of law.

8. GNI recently commissioned a report on reform options and the importance of ongoing political and financial investment in these critical law enforcement tools.[3] We are engaged in an ongoing dialogue with global companies, government agencies and other stakeholders to encourage the development of a transparent and efficient approach to cross-border law enforcement requests that includes robust protections for free expression and privacy.

9. The GNI is pleased to see that the draft Bill includes provisions to enable reformed MLATs and new international mutual assistance agreements. However, as noted above, we are concerned that the broad extraterritorial powers contained in the Bill and the likely consequences of the adoption of this approach by other governments may ultimately undermine the U.K. government's ability to conclude such agreements. We would invite the Committee to consider carefully the broader ramifications of enshrining such broadly framed and unilateral extraterritorial powers.

(III) Authorisation of bulk collection of communications and communications-related data

10. The GNI notes with disappointment that the draft Bill authorises U.K. government authorities to obtain warrants for the bulk interception of communications sent or received by persons outside the British Islands (sections 106 *et seq*.) and for the collection of communications data (sections 122 *et seq*.). As the GNI has previously expressed, bulk collection of communications data—both content and metadata—threatens privacy and freedom of expression rights and undermines trust in the security of electronic communications services provided by companies. This practice is incompatible with the principles of necessity and proportionality that the legal frameworks for communications surveillance must meet to ensure they are consistent with human rights standards. Rather than engaging in bulk collection, government surveillance programs should be particularised and based on individual suspicion, with independent judicial oversight that is adequately informed.

11. Furthermore, communications surveillance programs that involve bulk collection and are premised on distinguishing nationals from foreigners for increased privacy protections are unlikely to be effective. Both the UN Human Rights Committee and the Office of the UN High Commissioner for Human Rights have emphasised that any interference with the right to privacy must "comp[ly] with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance."[4]

(IV) Provisions that would weaken encryption technologies

12. The GNI is concerned that section 189(4)(c) of the Draft Investigatory Powers Bill creates broad powers for government authorities to undermine the use of encryption technologies. GNI members have contributed evidence to the Joint Scrutiny Committee on the importance of encryption for protecting the private communications and data of individuals and organisations. Advances in digital encryption have significantly improved security for individuals online, especially in financial transactions and communications. Encryption technologies are also important around the world for journalists, human rights defenders, persecuted minorities and people's representatives in parliaments and legislatures to be able to communicate confidentially.

13. A global digital economy will depend on user trust: trust that privacy and free expression rights are being protected, and trust that transactions and data are secure. Cybersecurity and network integrity are the foundations of this trust. The GNI recognises that all governments have a responsibility to protect national security and public safety. This important duty will increasingly involve improving the security of computers and networks, protecting citizens from cybercrime, and protecting children online. Government mandates that subvert or weaken digital security make individual users less safe, shrink the space for free expression and privacy and could slow the development and adoption of secure communications technologies. Deliberate undermining of security and encryption technologies also conflicts with legal requirements that companies and governments protect data from intrusion.[5]

(V) Absence of adequate mechanisms for transparency and accountability

14. As a member of the Freedom Online Coalition, the United Kingdom has made a commitment to promote "transparency and independent, effective domestic oversight related to electronic surveillance."[6] The GNI notes that the Draft Investigatory Powers Bill responds to recommendations that the United Kingdom make public a single law authorizing the surveillance of communications. At the same time, the Bill in its current form misses the opportunity to fulfill the state's commitment to greater transparency and accountability regarding its surveillance practices.

15. The GNI has recommended that governments disclose information about the surveillance demands they make on companies, including the number of surveillance demands, the number of user accounts affected by those demands, the specific legal authority for each of those demands, and whether the demand sought communications content or non-content or both. Companies should also be permitted to disclose the number of demands that they receive, how they respond to them, and the technical requirements for surveillance that they are legally bound to install, implement, and comply with. In addition to purely statistical data, governments should also make publicly available the laws and legal interpretations authorizing electronic surveillance, including executive orders, legal opinions that are relied on by executive officials, and court orders. GNI recommends that governments disclose to the victim that unlawful surveillance has taken place as soon as practical, as well as make public disclosures regarding the scope of unlawful surveillance and remedial and disciplinary actions taken.[7] This is consistent with the recommendations of Sir Nigel Sheinwald, who called on the U.K. government to "look at how it can improve transparency around the number and nature of our requests to domestic and overseas Communication Service Providers."[8]

16. Although sections 171 *et seq*. of the Bill contain some of the aforementioned safeguards, the GNI considers that mechanisms for transparency and public accountability regarding the conduct of communications surveillance are generally weak. Section 66(2) provides communications service providers with a "reasonable excuse" to disclose data requests to users, but this does not occur by default, and it remains an offence to disclose a warrant under other powers. We would urge the Committee to consider how users can have meaningful redress under the new oversight regime without transparency about authorised intrusions into their privacy.

Conclusion

17. The United Kingdom's policy debate leading up to the drafting of the current Investigatory Powers Bill has been watched closely by government and non-government actors around the world. The aforementioned reviews of David Anderson QC, Sir Nigel Sheinwald, and the Royal United Services Institute have set a high standard for public discussion, concurring that these government powers should be clearly set out in a single statute, should be transparent to users, and should raise standards for democratic and judicial oversight and provide a model for other jurisdictions. GNI welcomes changes to the Bill that meet these important recommendations.

18. We continue, however, to have serious concerns about the unilateral extra-territorial reach of laws outside of international legal structures and the precedent this sets for other governments. We remain very concerned about the provisions for bulk interception and collection of communications data, the level of transparency and accountability that the Bill sets for surveillance powers, and the impact on individuals if security and encryption standards are weakened. We are hopeful that this scrutiny process will highlight urgency for the United Kingdom to help create and encourage a responsible and sustainable global framework for global data for the long term. This framework should rely on the rule of law and uphold international standards for free expression and privacy.

19. The GNI is grateful for the opportunity to contribute to the important work of the Joint Committee. Our staff and membership are available to members to answer questions on our submission, and we will continue to offer a constructive and cross-sector collaborative forum for developing solutions that advance privacy and freedom of expression around the world.

Appendix A
The Global Network Initiative Principles
Preamble

These Principles on Freedom of Expression and Privacy ("the Principles") have been developed by companies, investors, civil society organizations and academics (collectively "the participants").

These Principles are based on internationally recognized laws and standards for human rights, including the Universal Declaration of Human Rights ("UDHR"), the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights ("ICESCR").[1,2]

All human rights are indivisible, interdependent, and interrelated: the improvement of one right facilitates advancement of the others; the deprivation of one right adversely affects others. Freedom of expression and privacy are an explicit part of this international framework of human rights and are enabling rights that facilitate the meaningful realization of other human rights.[3]

The duty of governments to respect, protect, promote and fulfill human rights is the foundation of this human rights framework. That duty includes ensuring that national laws, regulations and policies are consistent with international human rights laws and standards on freedom of expression and privacy.

Information and Communications Technology (ICT) companies have the responsibility to respect and protect the freedom of expression and privacy rights of their users. ICT has the potential to enable the exchange of ideas and access to information in a way that supports economic opportunity, advances knowledge and improves quality of life.

The collaboration between the ICT industry, investors, civil society organizations, academics and other stakeholders can strengthen efforts to work with governments to advance freedom of expression and privacy globally.

For these reasons, these Principles and their accompanying Implementation Guidelines establish a framework to provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of human rights globally.

The participants have also developed a multi-stakeholder governance structure to ensure accountability for the implementation of these Principles and their continued relevance, effectiveness and impact. This structure incorporates transparency with the public, independent assessment and multi-stakeholder collaboration.

The participants will seek to extend the number of organizations from around the world supporting these Principles so that they can take root as a global standard.

Freedom of Expression

Freedom of opinion and expression is a human right and guarantor of human dignity. The right to freedom of opinion and expression includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Freedom of opinion and expression supports an informed citizenry and is vital to ensuring public and private sector accountability. Broad public access to information and the freedom to create and communicate ideas are critical to the advancement of knowledge, economic opportunity and human potential.

The right to freedom of expression should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws or standards.[5] These restrictions should be consistent with international human rights laws and standards, the rule of law and be necessary and proportionate for the relevant purpose.[6, 7]

Participating companies will respect and protect the freedom of expression of their users by seeking to avoid or minimize the impact of government restrictions on freedom of expression, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication.

Participating companies will respect and protect the freedom of expression rights of their users when confronted with government[8] demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to information and ideas in a manner inconsistent with internationally recognized laws and standards.

Privacy

Privacy is a human right and guarantor of human dignity. Privacy is important to maintaining personal security, protecting identity and promoting freedom of expression in the digital age.

Everyone should be free from illegal or arbitrary interference with the right to privacy and should have the right to the protection of the law against such interference or attacks.[9]

The right to privacy should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws and standards. These restrictions should be consistent with international human rights laws and standards, the rule of law and be necessary and proportionate for the relevant purpose.

Participating companies will employ protections with respect to personal information in all countries where they operate in order to protect the privacy rights of users.

Participating companies will respect and protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards.

Responsible Company Decision Making

The implementation of these Principles by participating companies requires their integration into company decision making and culture through responsible policies, procedures and processes.

Participating companies will ensure that the company Board, senior officers and others responsible for key decisions that impact freedom of expression and privacy are fully informed of these Principles and how they may be best advanced.

Participating companies will identify circumstances where freedom of expression and privacy may be jeopardized or advanced and integrate these Principles into their decision making in these circumstances.

Participating companies will implement these Principles wherever they have operational control. When they do not have operational control, participating companies will use best efforts to ensure that business partners, investments, suppliers, distributors and other relevant related parties follow these Principles.[10, 11, 12]

Multi-stakeholder Collaboration

The development of collaborative strategies involving business, industry associations, civil society organizations, investors and academics will be critical to the achievement of these Principles.

While infringement on freedom of expression and privacy are not new concerns, the violation of these rights in the context of the growing use of ICT is new, global, complex and constantly evolving. For this reason, shared learning, public policy engagement and other multi-stakeholder collaboration will advance these Principles and the enjoyment of these rights.

Participants will take a collaborative approach to problem solving and explore new ways in which the collective learning from multiple stakeholders can be used to advance freedom of expression and privacy.

Individually and collectively, participants will engage governments and international institutions to promote the rule of law and the adoption of laws, policies and practices that protect, respect and fulfill freedom of expression and privacy.[13]

Governance, Accountability and Transparency

These Principles require a governance structure that supports their purpose and ensures their long term success.

To ensure the effectiveness of these Principles, participants must be held accountable for their role in the advancement and implementation of these principles.

Participants will adhere to a collectively determined governance structure that defines the roles and responsibilities of participants, ensures accountability and promotes the advancement of these Principles.

Participants will be held accountable through a system of (a) transparency with the public and (b) independent assessment and evaluation of the implementation of these Principles.

Annex A: Definitions

Freedom of Expression: Freedom of expression is defined using Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR):

UDHR: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

ICCPR: 1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Privacy: Privacy is defined using Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR):

UDHR: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

ICCPR: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.

Rule of Law: A system of transparent, predictable and accessible laws and independent legal institutions and processes which respect, protect, promote and fulfill human rights.

Personal Information: Participants are aware of the range of definitions for “personal information” or “personally identifiable information” and acknowledge that these definitions vary between jurisdictions. These Principles use the term “personal information” and interpret this to mean information that can, alone or in aggregate, be used to identify or locate an individual (such as name, email address or billing information) or information which can be reasonably linked, directly or indirectly, with other information to identify or locate an individual.

User: Any individual using a publicly available electronic communications service, for private or business purposes, with or without having subscribed to this service.

Best Efforts: The participating company will, in good faith, undertake reasonable steps to achieve the best result in the circumstances and carry the process to its logical conclusion.

Annex B: End Notes

[1] It is recognized that other regional human rights instruments address the issues of freedom of expression and

privacy, including: The European Convention, implemented by the European Court of Human Rights; the American Convention, implemented by the Inter-American Court of Human Rights and Inter-American Commission; and the Organization of African Unity, implemented by the African Commission on Human and People's Rights.

[2] These Principles have also been drafted with reference to the World Summit on the Information Society Tunis Agenda for the Information Society.

[3] It should be noted that the specific scope of these Principles is limited to freedom of expression and privacy.

[4] Taken from Article 19 of Universal Declaration of Human Rights and Article of 19 of the International Covenant on Civil and Political Rights. It should be noted that these Articles reference the right to "freedom of opinion and expression", and then describe the limited circumstances in which the right to "freedom of expression" (i.e. not opinion) can be restricted. That is the approach taken by these Principles.

[5] The narrowly defined circumstances should be taken from Article 19 of the International Covenant on Civil and Political Rights (ICCPR), namely the actions necessary to preserve national security and public order, protect public health or morals, or safeguard the rights or reputations of others. The scope of permissible restrictions provided in Article 19(3) of the ICCPR is read within the context of further interpretations issued by international human rights bodies, including the Human Rights Committee and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

[6] See Annex A for an illustrative definition of Rule of Law.

[7] These Principles have been drafted with reference to the Johannesburg Principles on National Security, Freedom of Expression and Access to Information. The Johannesburg Principles provide further guidance on how and when restrictions to freedom of expression may be exercised.

[8] Participating companies will also need to address situations where governments may make demands through proxies and other third parties.

[9] Taken from Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

[10] "Operational control" means the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity. This may be by contract, ownership of voting stock or representation on the Board of Directors or similar governing body.

[11] See Annex A for a definition of Best Efforts.

[12] It is recognized that the influence of the participating company will vary across different relationships and contractual arrangements. It is also recognized that this principle applies to business partners, suppliers, investments, distributors and other relevant related parties that are involved in the participating company's business in a manner that materially affects the company's role in respecting and protecting privacy and freedom of expression. The participating company should prioritize circumstances where it has greatest influence and/or where the risk to freedom of expression and privacy is at its greatest.

[13] It is recognized that participants may take different positions on specific public policy proposals or strategies, so long as they are consistent with these Principles.

The Global Network Initiative Implementation Guidelines

Purpose of This Document

The Principles on Freedom of Expression and Privacy (the "Principles") have been created to provide direction and guidance to the Information and Communications Technology ("ICT") industry and its stakeholders in protecting and advancing the enjoyment of these human rights globally.

These Implementation Guidelines provide further details on how participating companies will put the Principles into practice. The purpose of this document is to:

- Describe a set of actions which constitute compliance with the Principles.
- Provide companies with guidance on how to implement the Principles.
- As described in the accompanying Governance, Accountability and Learning Framework, each participating company will be assessed on their progress implementing the Principles after two years and annually thereafter.

The effectiveness of these Implementation Guidelines will be reviewed and assessed as experience in implementation of the Principles grows. The review process will include:

- Removing, revising or adding guidelines as appropriate.
- Considering the development of different versions of the Implementation Guidelines that may be tailored to specific regions or sectors.

Responsible Company Decision Making

Board Review, Oversight and Leadership
The Boards of participating companies will incorporate the impact of company operations on freedom of expression and privacy into the Board's review of the business.

The Board will:

- Receive and evaluate regular reports from management on how the commitments laid out in the Principles are being implemented.

- Review freedom of expression and privacy risk within the overall risk management review process.
- Participate in freedom of expression and privacy risk training as part of overall Board education.

Application Guidance: *"Board" could mean a Management Board or Executive Board if these are more appropriate for the participating company's structure.*

Human Rights Impact Assessments

Participating companies will employ human rights impact assessments to identify circumstances when freedom of expression and privacy may be jeopardized or advanced, and develop appropriate risk mitigation strategies when:

- Reviewing and revising internal procedures for responding to government demands for user data or content restrictions in existing markets
- Entering new markets, particularly those where freedom of expression and privacy are not well protected.
- Reviewing the policies, procedures and activities of potential partners, investments, suppliers and other relevant related parties for protecting freedom of expression and privacy as part of its corporate due diligence process.
- Designing and introducing new technologies, products and services.

The human rights impact assessments will be undertaken to different levels of detail and scope depending on the purpose of the impact assessment. However, participating companies should:

- Prioritize the use of human rights impact assessments for markets, products, technologies and services that present the greatest risk to freedom of expression and privacy or where the potential to advance human rights is at its greatest.
- Update human rights impact assessments over time, such as when there are material changes to laws, regulations, markets, products, technologies, or services.
- Draw upon resources from human rights groups, government bodies, international organizations and materials developed as part of this multi-stakeholder process.
- Include a consideration of relevant local laws in each market and whether the domestic legal systems conform to rule of law requirements.
- Utilize learning from real life cases and precedents.
- Focus on potential partners, investments, suppliers and other relevant related parties that are involved in the participating company's business in a manner that materially affects the company's role in respecting and protecting privacy and freedom of expression.
- Incorporate the outputs of human rights impact assessments into other company processes, such as corporate risk assessments and due diligence.

Partners, Suppliers and Distributors

Participating companies will follow these Principles and Implementation Guidelines in all circumstances when they have operational control.

When the participating company does not have operational control it will use best efforts to ensure that business partners, investments, suppliers, distributors and other relevant related parties follow the Principles.

Participating companies should focus their efforts on business partners, investments, suppliers, distributors and other relevant related parties that are involved in the participating company's business in a manner that materially affects the company's role in respecting and protecting freedom of expression and privacy. The participating company should prioritize circumstances where it has the greatest influence and/or where the risk to freedom of expression and privacy is at its greatest.

Application Guidance: *It is assumed that this approach will be taken in all relevant contracts signed after committing to the Principles and to all relevant pre-existing contracts.*

Application Guidance: *"Operational control" means the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity. This may be by contract, ownership of voting stock or representation on the Board of Directors or similar governing body.*

Application Guidance: *It is recognized that the influence of participating companies will vary across different relationships and contractual arrangements. See the definition of "best efforts" provided in Annex A.*

Integration into Business Operations

Participating companies will develop appropriate internal structures and take steps throughout their business operations to ensure that the commitments laid out in the Principles are incorporated into company analysis, decision making and operations.

Over time this will include:

Structure

The creation of a senior-directed human rights team, including the active participation of senior management, to design, coordinate and lead the implementation of the Principles.

Application Guidance: *This team may build on existing internal corporate structures, such as corporate social responsibility, policy, privacy or business ethics teams.*

Ensuring that the procedures related to government demands implicating users' freedom of expression or privacy rights are overseen and signed-off by an appropriate and sufficiently senior member of the company's management and are appropriately documented.

Procedures

Establishing written procedures that ensure consistent implementation of policies that protect freedom of expression and privacy and documenting compliance with these policies. Documentation of policies and compliance should be sufficiently detailed as to enable later internal and external review.

Establishing a means of remediation when business practices that are inconsistent with the Principles are identified, including meaningful steps to ensure that such inconsistencies do not recur.

Incorporating freedom of expression and privacy compliance into assurance processes to ensure compliance with the procedures laid out in the Principles.

Maintaining a record of requests and demands for government restrictions to freedom of expression and access to personal information.

Employees

Communicating the Principles to all employees, such as through the company intranet, and integrating the company's commitment to the Principles through employee training or orientation programs.

Providing more detailed training for those corporate employees who are most likely to face freedom of expression and privacy challenges, based on human rights impact assessments. This may include staff in audit, compliance, legal, marketing, sales and business development areas. Where appropriate and feasible, the orientation and training programs should also be provided to employees of relevant related

parties such as partners, suppliers and distributors.

Complaints and Assistance
Developing escalation procedures for employees seeking guidance in implementing the Principles.

Providing whistle-blowing mechanisms or other secure channels through which employees and other stakeholders can confidentially or anonymously report violations of the Principles without fear of associated punishment or retribution.

Application Guidance: *For example, each company might appoint or designate an internal ombudsman or auditor to monitor the company's business practices relating to freedom of expression and privacy.*

Freedom of Expression

Government Demands, Laws and Regulations
Participating companies will encourage governments to be specific, transparent and consistent in the demands, laws and regulations ("government restrictions") that are issued to restrict freedom of expression online.

Participants will also encourage government demands that are consistent with international laws and standards on freedom of expression. This includes engaging proactively with governments to reach a shared understanding of how government restrictions can be applied in a manner consistent with the Principles.

When required to restrict communications or remove content, participating companies will:

- Require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression.
- Interpret government restrictions and demands so as to minimize the negative effect on freedom of expression.
- Interpret the governmental authority's jurisdiction so as to minimize the negative effect on to freedom of expression.

Application Guidance: *It is recognized that the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time.*

- Seek clarification or modification from authorized officials when government restrictions appear overbroad, not required by domestic law or appear inconsistent with international human rights laws and standards on freedom of expression.

Application Guidance: *Overbroad could mean, for example, where more information is restricted than would be reasonably expected based on the asserted purpose of the request.*

- Request clear written communications from the government that explain the legal basis for government restrictions to freedom of expression, including the name of the requesting government entity and the name, title and signature of the authorized official.

Application Guidance: *Written demands are preferable, although it is recognized that there are certain circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written.*

- Adopt policies and procedures to address how the company will respond in instances when governments fail to provide a written directive or adhere to domestic legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.
- Challenge the government in domestic courts or seek the assistance of relevant government authorities, international human rights bodies or non-governmental organizations when faced with a government restriction that appears inconsistent with domestic law or procedures or international

human rights laws and standards on freedom of expression

Application Guidance: *It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on freedom of expression, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.****Application Guidance:*** *Policies and procedures adopted by participating companies will address situations where governments may make demands through proxies and other third parties to evade domestic legal procedures.*

Communications With Users

Participating companies will seek to operate in a transparent manner when required by government to remove content or otherwise limit access to information and ideas. To achieve this, participating companies will, unless prohibited by law:

- Clearly disclose to users the generally applicable laws and policies which require the participating company to remove or limit access to content or restrict communications.
- Disclose to users in a clear manner the company's policies and procedures for responding to government demands to remove or limit access to content or restrict communications.
- Give clear, prominent and timely notice to users when access to specific content has been removed or blocked by the participating company or when communications have been limited by the participating company due to government restrictions. Notice should include the reason for the action and state on whose authority the action was taken.

Privacy

Data Collection

Participating companies will assess the human rights risks associated with the collection, storage, and retention of personal information in the jurisdictions where they operate and develop appropriate mitigation strategies to address these risks.

Government Demands, Laws and Regulations

Participating companies will encourage governments to be specific, transparent and consistent in the demands, laws and regulations ("government demands") that are issued regarding privacy online.

Participating companies will also encourage government demands that are consistent with international laws and standards on privacy. This includes engaging proactively with governments to reach a shared understanding of how government demands can be issued and implemented in a manner consistent with the Principles.

Participating companies will adopt policies and procedures which set out how the company will assess and respond to government demands for disclosure of personal information. When required to provide personal information to governmental authorities, participating companies will:

- Narrowly interpret and implement government demands that compromise privacy.
- Seek clarification or modification from authorized officials when government demands appear overbroad, unlawful, not required by applicable law or inconsistent with international human rights laws and standards on privacy.

Application Guidance: *Overbroad could mean, for example, where more personal information is requested than would be reasonably expected based on the asserted purpose of the request.*

- Request clear communications, preferably in writing, that explains the legal basis for government demands for personal information including the name of the requesting government entity and the name, title and signature of the authorized official.

Application Guidance: *Written demands are preferable, although it is recognized that there are certain*

circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written.

- Require that governments follow established domestic legal processes when they are seeking access to personal information.
- Adopt policies and procedures to address how the company will respond when government demands do not include a written directive or fail to adhere to established legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.
- Narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that Country.

Application Guidance: *It is recognized that the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time.*

- Challenge the government in domestic courts or seek the assistance of relevant authorities, international human rights bodies or non-governmental organizations when faced with a government demand that appears inconsistent with domestic law or procedures or international human rights laws and standards on privacy.

Application Guidance: *It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on privacy, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.*

Application Guidance: *Policies and procedures adopted by participating companies will address situations where governments may make demands through proxies and other third parties to evade domestic legal procedures.*

Communications with Users

Participating companies will seek to operate in a transparent manner when required to provide personal information to governments. To achieve this, participating companies will:

Application Guidance: *Participating companies will work with the Organization to raise awareness among users regarding their choices for protecting the privacy of their personal information and the importance of company data practices in making those choices.*

- Disclose to users in clear language what generally applicable government laws and policies require the participating company to provide personal information to government authorities, unless such disclosure is unlawful.
- Disclose to users in clear language what personal information the participating company collects, and the participating company's policies and procedures for responding to government demands for personal information.
- Assess on an ongoing basis measures to support user transparency, in an effective manner, regarding the company's data collection, storage, and retention practices.

Multi-stakeholder Collaboration

Engagement in Public Policy

Participants will encourage governments and international institutions to adopt policies, practices and actions that are consistent with and advance the Principles.

Individually or collectively participants will:

- Engage government officials to promote rule of law and the reform of laws, policies and practices

that infringe on freedom of expression and privacy.

Application Guidance: *Promoting rule of law reform could include rule of law training, capacity building with law-related institutions, taking public policy positions or external education.*

- Engage in discussions with home governments to promote understanding of the Principles and to support their implementation.
- Encourage direct government-to-government contacts to support such understanding and implementation.
- Encourage governments, international organizations and entities to call attention to the worst cases of infringement on the human rights of freedom of expression and privacy.
- Acknowledge and recognize the importance of initiatives that seek to identify, prevent and limit access to illegal online activity such as child exploitation. The Principles and Implementation Guidelines do not seek to alter participants' involvement in such initiatives.
- Participants will refrain from entering into voluntary agreements that require the participants to limit users' freedom of expression or privacy in a manner inconsistent with the Principles. Voluntary agreements entered into prior to committing to the Principles and which meet this criterion should be revoked within three years of committing to the Principles.

Application Guidance: *It is recognized that participants may take different positions on specific public policy proposals or strategies, so long as they are consistent with these principles.*

Internal Advisory Forum
A confidential multi-stakeholder Advisory Forum will provide guidance to participating companies on emerging challenges and opportunities for the advancement of freedom of expression and privacy.

External Multi-stakeholder Learning Forums Participants will promote global dialogue and understanding of the Principles and share learning about their implementation. Participants will engage with a broad range of interested companies, industry associations, advocacy NGOs and other civil society organizations, universities, governments and international institutions.

Participants will create a global learning, collaboration and communication program. This program will identify stakeholders, topics and forums for learning, collaboration and communication activities.

Application Guidance: *This could include, for example, the Internet Governance Forum, the International Telecommunications Union, the UN Global Compact and the UN Special Representative of the Secretary General on human rights and transnational corporations and other business enterprises.*

Part of this learning program will be an annual Multi-stakeholder Learning Forum focusing on the rights to freedom of expression and privacy, the specific scenarios in which these rights are affected and other broader issues related to the implementation of the Principles.

Where participants have activities or operations in the same countries they will seek to collaborate on the development of local dialogues on relevant prominent issues and emerging concerns in those localities.

Participants will develop and share innovative tools, resources, processes and information that support the implementation of the Principles.

Included in the learning program will be a consideration of the role that tools such as encryption, anonymizing technologies, security enhancements and proxy technologies can play in enabling users to manage their media experiences and protect freedom of expression and privacy.

Governance, Accountability & Transparency

Governance
A multi-stakeholder representative Board will oversee this initiative, described in more detail in the accompanying Governance, Accountability and Learning Framework document.

Reporting on Implementation
There will be three different levels of reporting on the progress being made to implement the Principles, described in more detail in the accompanying Governance, Accountability and Learning Framework document.

Independent Assessment
There will be a system of independent assessment of the implementation of the Principles, described in more detail in the accompanying Governance, Accountability and Learning Framework document.

Annex A: Definitions

Freedom of Expression: Freedom of expression is defined using Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR):

UDHR: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

ICCPR:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
(a) For respect of the rights or reputations of others;
(b) For the protection of national security or of public order (ordre public), or of public health or morals.

Privacy: Privacy is defined using Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR):

UDHR: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

ICCPR:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

Rule of Law: A system of transparent, predictable and accessible laws and independent legal institutions and processes, which respect, protect, promote and fulfill human rights.

Personal Information: Participants are aware of the range of definitions for “personal information” or “personally identifiable information” and acknowledge that these definitions vary between jurisdictions. These Implementation Guidelines use the term “personal information” and interpret this to mean

information that can, alone or in aggregate, be used to identify or locate an individual (such as name, email address or billing information) or information which can be reasonably linked, directly or indirectly, with other information to identify or locate an individual.

User: Any individual using a publicly available electronic communications service, for private or business purposes, with or without having subscribed to this service.

Best Efforts: The participating company will, in good faith, undertake reasonable steps to achieve the best result in the circumstances and carry the process to its logical conclusion.

Appendix B
Participants in the Global Network Initiative

ICT Companies

Facebook
Google
LinkedIn
Microsoft
Procera Networks
Yahoo!

Academics

Berkman Center for Internet and Society, Harvard University
Center for Business and Human Rights, New York University Stern School of Business
Centro de Estudios en Libertad de Expresión, Universidad de Palermo (Argentina)
Deirdre Mulligan, University of California at Berkeley School of Information
Ernest Wilson, Annenberg School for Communication, University of Southern California
George Washington University Law School
Kyung-Sin Park, Korea University Law School
Nexa Center for Internet and Society, Politecnico di Torino (Italy)
Philip N. Howard, University of Washington and Central European University
Rebecca MacKinnon, New America Foundation
Research Center for Information Law, University of St. Gallen (Switzerland)

Civil Society Organizations

Bolo Bhi
Center for Democracy and Technology
Centre for Internet and Society
Committee to Protect Journalists
Human Rights First
Human Rights in China
Human Rights Watch
Index on Censorship
Institute for Reporters' Freedom and Safety
International Media Support
Internews
PEN American Center
World Press Freedom Committee

Investors

Boston Common Asset Management
Calvert Investments
Church of Sweden
Domini Social Investments
EIRIS Conflict Risk Network
F&C Asset Management
Folksam
Trillium Asset Management
Walden Asset Management

21 December 2015

---

[1] Global Network Initiative, 'Written Evidence to the Communications Data Bill Joint Scrutiny Committee', 23 August 2012, available at http://www.globalnetworkinitiative.org/sites/default/files/GNI%20submission%20on%20U.K.%20comms%20data%20bill%2023%20August%202012.pdf; Open Letter to Prime Minister David Cameron regarding the Data Retention and Investigatory Powers Bill, 14 July 2014, available at http://www.globalnetworkinitiative.org/sites/default/files/GNI%20Open%20Letter%20to%20U.K.%20Prime%20Minister%20-%20July%202014.pdf.

[2] See, e.g., sections 31, 69 (referring to communications data), 79 (referring to data retention), 100 (referring to equipment interference), 108 (referring to bulk interception), 116(3), 130(3) (referring to bulk acquisition), and 145(3).

[3] Andrew K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, The Global Network Initiative (2015), available at: https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf.

[4] Human Rights Committee, Concluding observations on the fourth report of the United States of America, CCPR /C/USA/CO/4 (2014), para. 22; 'The right to privacy in the digital age', Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37 (2014) para. 36.

[5] See, e.g., **Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Article 4; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 17; see also, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 2013/0027 (COD).**

[6] Recommendations for Freedom Online, adopted in Tallinn, Estonia, on April 28, 2014 by Ministers of the Freedom Online Coalition ('Tallinn Agenda').

[7] Global Network Initiative, 'Getting Specific about Transparency, Privacy, and Free Expression Online', November 5, 2014, available at: http://www.globalnetworkinitiative.org/news/getting-specific-about-transparency-privacy-and-free-expression-online.

[8] Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing, Sir Nigel Sheinwald, available at: https://www.gov.U.K./government/uploads/system/uploads/attachment_data/file/438326/Special_Envoy_work_summary_final_for_CO_website.pdf.