The Aspen IDEA Plan for a Common Digital Market of Goods, Services and Ideas

September 12, 2011

TABLE OF CONTENTS

SECTION A

The Aspen IDEA Implementation Plan for a Common Digital Market of Goods, Services and Ideas

The Aspen IDEA Implementation Plan for a Common Digital Market of Goods, Services and Ideas

The Internet is the richest medium in human history for the exchange of information and commerce. Two billion people around the globe are now connected. Within the next decade or two, nearly everyone on the planet will be a part of a single common platform with unparalleled potential for personal fulfillment, economic growth and social change.

An unfettered flow of communications across borders is essential to the well-being of virtually every country, business and individual in the world. Yet new forces of fragmentation, repression, and disregard for fundamental rights of property, security, privacy and human rights are challenging the future of this common medium. Some countries are giving preferential treatment to goods and services from domestic companies. Some restrict full use of the Internet by their citizens. Some avoid fair and inclusive processes as they develop policies affecting digital commerce. Some state actors and non-state actors do not honor and respect in all appropriate ways fundamental rights of property and individuals, as each are asserted and expressed in the medium of the global Internet. Taken together, the various departures from the widely understood values and practices of the Internet threaten to block its future development and deny the world the benefit of a common medium.

Everyone wants to see the Internet reach its global potential. But it is widely agreed that the Internet has flourished with governance through multistakeholder organizations, as opposed to being ruled by patchworks of national law or an international agreement. As reflected most recently by the OECD communiqué relating to the Internet, there is broad consensus among governments, firms, and members of civil society that the Internet's future governance requires respect for national sovereignty over various important topics, as well as reliance on the Internet community itself to engage in self-governance.

Contemporaneous with, and in purposeful accord with, the process that culminated in the OECD communiqué, the Aspen IDEA Project created a coherent body of values and beliefs about the Internet: a description of the culture of the Internet that most wish to perpetuate. The Aspen IDEA participants called that effort the Common Statement and Principles ("Principles"). They are set forth in Sections B and C.

The next step then is to take this consensus about governance and culture into the realm of implementation. The Principles created by the Aspen IDEA participants are the substantive foundation of this implementation plan. To this end, the Aspen IDEA team proposes a method for facilitating the governance of the Internet.

The plan has two basic design principles: (1) maintenance of national sovereignty (hence the Plan does not depend on treaty-based governance), and (2) maximizing the use of expert, pragmatic, and efficient multistakeholder organizations for accomplishing many of the goals of regulation and standard setting that in other sectors of commercial and individual activity are sometimes undertaken by expert associations, industry groups, or government agencies.

Summary of the Plan

Governments would each enter into an identical contract with a newly formed non-governmental multistakeholder organization, called the Protocol Certification Organization (PCO). The PCO would foster, financially support, and assure the reasonable performance of various expert international multistakeholder organizations, each organized around one or more of the subject matter topics addressed by the Principles. These are called subject matter multistakeholder organizations (SMOs). The SMOs would engage in setting standards and guidelines for behavior, certify companies as complying with national policies, certify countries as having national policies that comport with the Principles, and reach reasoned conclusions on any disputes brought to them.

If an SMO certifies a company as complying with the policies of a contracting government, then by the terms of a government's contract with the PCO, that country would treat such a certified company just as it would treat all other companies in its jurisdiction – it would adhere to a non-discrimination principle.

Parties aggrieved by an SMO's decision could appeal to the PCO. It would rule on the reasonableness of the SMO's decision-making. In the event that the PCO ratified an SMO's decision (i) that a government failed to adopt national policies that accorded with the Principles or (ii) that a company was not acting in accord with a nation's policies, the PCO would then report that decision to all the contracting governments. This is sometimes called a "name and shame" enforcement mechanism.

Further Explanation

The PCO would be a non-governmental multistakeholder entity funded by companies, foundations and contracting nations. Each government would have to agree with the PCO (not with each other) to:

1. Adopt national policies that are consistent with the Principles and adhere to the procedural Boundary Conditions described below and set forth in more detail in Section D.

2. Provide for the participation in the government's own process of implementing national rules regarding Internet governance.

3. Follow processes for adopting and enforcing such national policies that are within certain broadly defined boundary conditions, such as timeliness, transparency, non-arbitrary conduct and "least trade restrictive" formulations of policies.

4. Treat in a non-discriminatory way all companies certified by the SMOs (as set forth below).

5. Respond in a reasoned, transparent manner to all legitimate reports received by the PCO of the government's non-compliance or the non-compliance of its companies.

In the government-PCO contract, each signatory government would maintain the right under extraordinary circumstances to suspend its promise to recognize the subject matter certifications of the SMOs. However it would have to agree to:

6. Explain any opt-out of the non-discrimination principle in a reasoned manner, and terminate the opt-out after a defined period of time, or renew it with an additional reasoned explanation.

For its part, the PCO would agree with each government that it will:

1. Operate under a multistakeholder governance arrangement.

2. Certify as many SMOs as are necessary for addressing all the Principles. Presumptively the jurisdictions of the SMOs would be collectively exhaustive and mutually exclusive.

3. Provide adequate funding to SMOs where needed to assure adequate governance and performance.

4. Review complaints, reason transparently and fairly as to all matters, and report in a timely matter its decisions to all governments with which it has contracted and conduct itself transparently, efficiently, and in a manner focused on assuring good processes.

5. Assure signatory countries that each certified SMO will, within the ambit of topics it is certified to address:

    - adhere to multistakeholder governance.
    - utilize sufficient expertise to fulfill its mission.
    - operate by methods likely to produce reasonable outcomes.
    - set standards where relevant.
    - determine best practices for conduct by firms, NGOs and individuals using the Internet.
    - receive applications from companies seeking to be certified as in compliance with the policies of any particular nation, and after reasoned deliberation determine whether to certify such companies as complying with any particular government's policies (thereby creating the presumption of non-discrimination that would be presented to the signatory nation, in accordance with the government's contract with the PCO).
    - receive complaints about countries or companies, and reach reasoned conclusions about such complaints (leading potentially to the "naming and shaming" mentioned above).

The SMOs will be primarily responsible for the work of facilitating global digital commerce. In them will reside the expertise, deliberative processes, and open decision-making that has largely characterized the growth of the Internet over the last 20 years. Many if not most of the SMOs will be organizations that already exist or versions of such organizations.

Benefits of the Plan

This plan is intended and designed to appeal to governments, companies, and civil society representatives for at least the following reasons:

<u>Governments:</u>

1. Can delegate to the SMOs much of the detailed standard setting and dispute resolution that is the burdensome part of governance.

2. Can treat the PCO as a single point of contact, avoiding the appearance of controlling or influencing the SMOs, and simplifying contractual performance.

3. Will reserve all national sovereignty powers, including determining that any firm is in compliance with its laws and regulations. Under the contract it agrees to non-discrimination, unless it opts-out of such agreement.

4. Will tend to anchor their national policies around the Principles because the PCO contract provides a mechanism to elevate their stature beyond purely voluntary efforts.

Companies:

1. Will have in the SMOs centralized forums in which to seek certifications of compliance as to all national policies relevant to the company.

2. Will benefit from the SMOs' understanding of the substance, and differences among, national policies, because the SMOs are relied upon in the implementation process as a result of the contract between governments and the PCO.

3. Will more readily obtain global reach because of the presumptive condition of non-discrimination after certification, as set by the contract between a signatory nation and the PCO.

Civil Society:

1. Will be assured of seats at the table where both process and substance of governance of the Internet will be determined.

2. Will be appropriately supported and welcomed by all participants.

3. Will be provided with some funding by the PCO for civil society participation in the process.

This plan does not limit any rights that civil society members otherwise may have to affect the laws or regulations of any nation.

SECTION B

Aspen IDEA Common Statement

The Aspen IDEA Common Statement

An integral part of Aspen IDEA's efforts to define international principles, norms, and rules for the global Internet has been the discussion and formulation of the Aspen IDEA Common Statement. The Common Statement provides the organizing principle and starting point for efforts to develop more specific Internet principles. It also guides the Implementation Plan outlined in this paper.

The Common Statement has been the subject of extensive discussion and analysis. It was first formulated in March 2011 in response to the efforts of the original Working Groups and in response to discussions in Washington and Los Angeles during the October 2010 to March 2011 period. This was prior to the time many of our European and other international colleagues joined the Aspen IDEA effort. Subsequent to the March 2011 Brussels meeting, the initial draft of the Common Statement was discussed, debated and refined in all three of the reformulated and expanded Working Groups. The Common Statement now reads as follows:

> *All elements of a digital economy and society should be bought, sold, created, or experienced in a single seamless global market of goods, services, and ideas over broadband infrastructures that operate in a dynamic commercial environment.*
>
> *All information should be transferred across any and all national borders as senders and receivers should wish. Any restrictions resulting from measures taken by governments to safeguard public policy principles should be proportional, transparent, equitable, necessary, provided for by law, and consistent with international treaties or best practices on privacy, security, protection of intellectual property rights, and free expression. Commercial agreements and voluntary arrangements may go beyond measures taken by governments but should be compliant with applicable law, relevant international treaties, and best practices.*
>
> *The seamless, global transfer of information and exchange of digital goods and services should occur in a responsible and accountable trusted environment that guarantees the interests of national and personal security, the right of individuals to privacy, and the interests individuals and firms have in rights of property and rights of access to information, association, and free expression.*

The mandate of each Post-Brussels Working Group and their modifications to the original Common Statement are described below. These very brief summaries are not intended to and do not do justice to the full discussions that occurred during the course of the many calls and meetings.

Working Group 1
Market Access

This Working Group focused on the first paragraph of the Common Statement. It took as its major objective the creation of a seamless global digital market.

The Working Group discussed the importance of the connectivity component of the Internet and the challenges that require regulatory flexibility to allow for new business models and new services and offerings in a broadband world. Participants noted that governments have a legitimate role in enabling the digital economy, but there is a need to set limits on what government does and how it does it. Notions of least trade restrictive, transparency and due process, global standards and norms were proposed. The participants also thought it important to make the Common Statement attractive to developing countries and to recognize the legitimate aspirations of governments and civil society to foster economic development, cultural diversity and freedom of expression.

Working Group 2
Free Flow of Cross Border Information

This Working Group focused on the second paragraph of the Common Statement. In particular, it looked at issues relating to cloud computing and jurisdictional and other issues which affect the flow of information across borders.

The Working Group discussed the need to explicitly recognize human rights and the rule of law. There was recognition that governments have a right to intervene in matters such as security, privacy and crime prevention. But the Group noted that restrictions resulting from measures taken to safeguard public policy principles should be proportional, transparent, equitable, necessary, provided for by law and consistent with international standards. The Group noted that the IDEA participants are attempting to design a process where governments exercise their rights in a narrow way. Participants agreed that while governments are sovereign, that sovereignty is affected by, for example, binding international trade and other agreements.

Working Group 3
Trusted Environment

This Working Group focused on the third paragraph of the Common Statement. It debated issues involving supporting a global Internet where information, digital goods and digital services flow freely in a trusted environment, one in which privacy, security, and rights of expression and property are respected.

Participants pointed out that there were inherently different “worldviews” on various issues, particularly when drilling down to specifics on freedom of expression, intellectual property protection, intermediary liability, and so on. The terms “lawful” and “rule of law” were brought up as examples of terms that are frequently disputed, and the Group discussed suggestions on how to address different views with respect to those terms and the issues they encompass. The Group also discussed privacy, where the U.S. and Europe have diverged, and intermediary liability, which has proven to be a difficult concept to address in the past. Participants noted that the original Statement missed certain elements, such as the recognition of human rights and rule of law as a foundation for activity on the Internet. In a discussion of multistakeholder institutions, participants discussed the need for open participation, inclusion of civil society, transparency, due process, and respect for the rights of users and existing legal arrangements.

SECTION C

Aspen IDEA Principles

The Aspen IDEA Principles

Background

For at least the last decade, industry, civil society and governments have engaged in a serious and concerted attempt to develop a consistent set of principles relating to the governance and operation of the global Internet. As Reed Hundt, Chairman of the Aspen IDEA Project, noted in a recent article:

> *A critical job for everyone concerned with the Internet now is to determine the form of such governance. This is not harder than, or less important than, the era of Republic creation that in Atlantic nations stretched from the late 18th century to the mid-19th century. It just needs to happen at 21st century speed – we have not a moment to lose.*

There has been no shortage of efforts in this area. Recent examples include the work of the Internet Governance Forum, the U.S.-EU Trade Principles for ICT, the EU's Digital Agenda for Europe and the June 2011 OECD Communiqué on Principles for Internet Policy-Making. Attached as Section F is a chart, originally prepared by Steve Stewart of IBM and revised by Shanti Kalathil of Aspen IDEA, substantively comparing several of these recent projects.

A major task for the Internet community is to ensure that the many efforts are consistent and converge in a meaningful way. This challenge is particularly difficult for Internet civil society participants due to funding and other resource constraints. Moreover, there continues to be debate as to whether such principles should be "soft" recommendations or adopted in some more binding fashion. See Harold Koh's "Why Do Nations Obey International Law?" 106 Yale L.J. 2599 (1997).

As noted above, an important recent effort is the June 2011 OECD Communiqué. There the OECD produced a set of broad principles for safeguarding the open Internet and addressed several key international threats. See Washington Post OpEd, July 8, 2011, by Karen Kornbluh and Daniel Weitzner. An important group of civil society participants had reservations about several of the OECD Principles. See CSISAC Statement of June 2011.

The Aspen IDEA Contribution

This background provides important context for the Aspen IDEA efforts to develop a set of Internet principles. The Aspen IDEA Principles, along with the Common Statement, provide the substantive basis for the Implementation Plan outlined in Section A of this paper. As noted in the Plan, these Principles are to be embodied in binding legal instruments.

As with the Common Statement, the IDEA Principles were first formulated in March 2011 in response to the efforts of the original Working Groups and in light of discussions in Washington and Los Angeles. Subsequent to the March 2011 Brussels meeting, when many of our international colleagues joined the Project, the Principles were discussed, debated and refined in the three reformulated and expanded Working Groups.

The resulting Principles are set forth below and arranged by Working Group. They are the Principles as discussed and debated through August 2011, with the following two sets of modifications. The first group of minor changes is to more closely align the IDEA Principles with the OECD Principles. (The edits also attempt to take account of the concerns raised by civil society mentioned above.) The second set of modifications add several additional principles to the list in order to address market and market access

related issues. The Aspen IDEA staff welcomes comments on any of these modifications and the Principles in general between now and the Washington, D.C. Plenary Meeting November 1-2.

The Principles

The Principles are to be embodied in a binding legal instrument, to add credibility and a new focal point for market governance. The Principles fall into three clusters: those that strengthen the Internet infrastructure and promote free trade in the Internet's ecosystem; those that enhance the international free flow of information; and those that promote a trusted environment for the Internet.

A. Strengthen the Internet Infrastructure and Promote Free Trade in the ICT Ecosystem

1. Governments should foster a precompetitive policy environment and promote investment, including cross-border investment, in the facilities and services supporting the Internet infrastructure and expansion of the Internet as rapidly as possible.

2. Governments should expand the Internet by encouraging competition in broadband access and other relevant markets. In light of the growing importance of broadband mobile networking, governments should commit to embrace policies that:

    a. maximize the availability of spectrum through continual improvements in spectrum policy,

    b. assure technology neutrality in the design of the wireless network and its devices, and, subject to competition policies,

    c. permit commercially determined approaches to the intersection of the wired and wireless segments of the Internet space.

3. To permit suppliers of communications infrastructure to participate fully in the ICT ecosystem, and thus fuel investment in that infrastructure, governments should commit to:

    a. redefine the relevant market for networked consumer information to provide nondiscriminatory treatment of telecom carriers in regard to privacy requirements for how they handle customers' electronic data,

    b. establish frameworks for intercarrier peering that allow for differential pricing based on substantial differences in traffic loads and failure to adhere to reasonable, non-discriminatory practices in regard to network security, and subject to periodic review of competition authorities,

    c. establish flexibility for network pricing and traffic policies for carriers that offer a "base line" service featuring reasonable price, speed, quality of service, and data caps to all customers.

4. Governments should expand the capability of the Internet to increase trade and adopt policy measures designed to maximize free trade in all aspects of the ICT ecosystem.

5. To encourage trade and innovation in services and software, governments should allow:

    a. IP-based and converged services (e.g., cloud computing and environmental services) to enjoy maximum regulatory flexibility, and be subject to regulatory obligations only to the extent that they are narrowly tailored to the dynamics of this rapidly evolving sector.

b. Governments also should reinforce policies that support technology neutrality, including promoting digital product neutrality for applications and software.

6. As the range of ICT applications expand in the economy and society, and the salience of these applications to important rights and needs of citizens increases, new policy interventions are needed in ICT market. Governments should make best efforts to advance "regulatory coherence" among national policies with major impact on ICT markets, including by creating internal government mechanisms to promote coherence. To do so governments should publish annually a list of planned future measures that impact ICT goods and services.

B. Free Flow of Information Principles

1. Governments should allow the free flow of information globally.

    a. Allowing information to move freely and be stored globally permits the capture of economies of scale and makes it possible to reap the economic benefits associated with the Internet.

2. Facilities and information storage.

    a. Artificially limiting the location of data geographically reduces the resiliency of the Internet and undermines its stability.

    b. Governments should not require that facilities or information be located in a specific country or region.

3. Other Protections.

    a. Freedom of expression, as defined in international treaties on human rights, should be preserved.

    b. Any government restrictions on content should be transparent, necessary, provided for by law, and consistent with international standards on free expression and privacy.

    c. Governments should provide information on the Internet the same protection from government access as information stored locally or housed in any other environment.

    d. To encourage the online dissemination of services and content, governments should offer providers appropriate intermediary safe harbors to shield them when hosted content or software is alleged to violate a law or infringe on third party rights, including intellectual property rights.

C. Creating a Trusted Environment

1. Global Internet policy and practice must promote a functioning 'trusted environment' with respect to issues such as security, privacy, intellectual property rights, protection of children, consumers, and personal data online, and free expression. All stakeholders should recognize government, civil society and private sector needs for security of the Internet.

    a. Governments should implement clear, transparent, and impartial laws, including due process protections and reasonable notice, to govern requests for third party information stored by Internet providers.

b. Governments should develop fast, efficient methods for gathering and sharing information regarding fraudulent and deceptive commercial practices that can victimize consumers through the Internet, and the means to deter, detect, and prevent such practices.

c. Governments should develop policy requirements that make certain that consumers' personal data is portable. Such policies should provide consumers with reasonable access to data gathered by suppliers about users' conduct on the Internet (e.g., records of past purchases) and personal information submitted to Internet-based applications (e.g., personal health information stored on a web-based application for personal health monitoring).

d. Governments have an obligation to assure that the private sector maintains enhanced consumer protection, including:

    i. Internet providers should transparently explain their information handling practices and the regulatory needs of their server locations with respect to such issues as data protection and privacy.

    ii. Internet providers should disclose requested third-party information only to the extent required by law and, to the extent permitted by law, should provide affected customers with reasonable advance notice of any such compelled disclosure.

    iii. Governments should work to create a level playing field and achieve global interoperability on privacy and data protection principles by basing privacy rules on globally recognized principles (such as the OECD privacy guidelines) and by extending mutual recognition of laws that achieve the same objectives. Privacy rules should also consider fundamental rights such as freedom of speech, freedom of the press, and an open and transparent government.

e. Governments should enforce intellectual property rules as they relate to the Internet and the ICT ecosystem.

f. Governments should ensure clearly defined legal rights and a robust and fair process to protect rights, including users' rights, consistent with the need of governments to enforce applicable law. Governments, industry and civil society should work together to foster respect for the rule of law, defined here as a system of transparent, predictable and accessible laws and independent legal institutions and processes which respect, protect, promote and fulfill human rights.

g. Governments should implement internationally recognized, market-driven security standards and best practices to promote cybersecurity, while simultaneously ensuring that the framework conditions ensuring an open Internet are not disrupted.

SECTION D

Aspen IDEA Boundary Conditions

Aspen IDEA Boundary Conditions

Contracting Governments agree to the following process when establishing policies:

1. Contracting Governments will modify or create policies necessary to achieve these principles in a timely manner.

2. Contracting Governments will follow best practices to achieve transparency in policymaking, including giving timely public notice and comment when formulating policies. They will make all policies publicly available and ensure that enforcement and implementation decisions are transparent.

3. Transparency provisions will include all instructions to state-owned enterprises on how to implement policies.

4. Contracting Governments will embrace a system that allows expert SMOs, as certified by the PCO, to help formulate standards and practices to implement national policies and certification methods.

5. Contracting Governments will provide expedited consideration of parallel enforcement actions against any entity (e.g., a company) that violates the Principles significantly in their territories.

6. Contracting Governments have the right, under extraordinary circumstances, to exercise opt-out rights. Governments could suspend their recognition of certifications from a particular SMO for a limited period of time after giving thorough public explanations.

The Protocol Certification Organization ("PCO") agrees to follow additional governance guidelines as follows:

1. The PCO will consist of a board of non-governmental experts that is representative of the Contracting Governments.

2. No more than two-thirds of the PCO's Board may be from the private sector. To maintain representation from stakeholders outside of the private sector, it may be necessary to waive membership dues for some board members.

3. The PCO shall adopt a reasonable rule about timeliness of decisions.

4. The PCO shall develop voting rules such that no single individual board member or small group of board members can hold veto power.

5. The PCO will establish a technical advisory board that is widely open to experts from all countries, whether or not they are Contracting Nations.

6. The PCO will follow best practices to achieve transparency in its decision-making, including notice and an opportunity for comment when certifying proposed standards and best practices from SMOs.

7. The PCO will have a clear procedure for appeals.

Subject Matter Multistakeholder Organizations ("SMOs") agree to follow additional governance guidelines as follows:

1. SMOs will be headquartered in a Contracting Nation and open to membership by members of civil society from all Contracting Nations.

2. SMOs may charge membership fees to cover the costs of their activities.

3. SMOs will commit that expertise is the primary qualification for membership.

4. SMOs will embrace a transparent process even while decision-making processes may differ.

5. SMOs will embrace due process and respect for existing legal procedures.

SECTION E

Stress Tests

Aspen IDEA Project - Stress Tests

The IDEA Plan contemplates a process where governments contract with the Protocol Certification Organization (PCO) to abide by the IDEA Principles and respect the Boundary Conditions; where a company applies to the Subject Matter Multistakeholder Organizations (SMO) on particular topics for certification that the company complies with the standards of a particular contracting country, and, if certified, is treated as a national company in that country; and where others can bring complaints to the SMO that a company or country is not following the IDEA Principles. As such, the design would lead to the following answers to questions below.

1. **Q: Is this proposal consistent with trade obligations, especially Most Favored Nation?**

   A: Yes. It is not a trade agreement. This Implementation Plan creates a common set of Principles that reduce uncertainty about the policy environment of contracting nations and introduces an expedited method for companies to be certified as being compliant with national policies. It also introduces a major role for multistakeholder organizations in shaping the implementation of Internet related policies, a form of pragmatic reliance on expertise that is a hallmark of Internet governance at its best.

2. **Q: Suppose the European Union adopted additional privacy provisions beyond those selected by the United States, both signatories, what happens?**

   A: The Principles provide common anchors for policy, and create a process of collaboration that should lead to more uniformity over time. But, the Principles are not expected or intended to lead to complete policy harmonization. Assuming that U.S. privacy policies conform to the Principles, there is nothing that hampers the EU from requiring additional protections, so long as they meet general boundary conditions – e.g., they are least trade restrictive. The SMO for privacy would need to assure that the certification process could distinguish between U.S. and EU requirements in order to respect both systems.

3. **Q: If an SMO determines that the policy implementation of the Principles by a contracting government was inconsistent, what could it do?**

   A: National policy is the domain of governments. A key purpose of this Implementation Plan, to the extent possible, is to move to an expert dominated system whose participants understand the benefits of common global principles. But if an SMO received a petition, it might determine that a contracting nation's policies are not consistent with that Principle. The determination could be reviewed by the PCO. If sustained by the PCO, the determination would be reported by the PCO to all contracting governments.

4. **Q: Suppose China is not a contracting country, could a global Chinese firm such as Huawei benefit from the Principles and the certification system?**

A: A company has to seek certification from an SMO in a contracting country. Therefore, if China were not a contracting country, then Huawei could participate only if it had major production activities in a contracting country, say, Canada. It could then, on behalf of its Canadian business only, seek certification of its conduct by petitioning the relevant SMO. If successful, it would then obtain the benefit of non-discrimination as to the activities of that Canadian entity in Canada. The hope would be that having experienced the benefits of this process, Huawei would then advocate that other Chinese firms and Chinese policy move towards compliance with the IDEA Principles. If on the other hand, Huawei were found not to be in compliance, it would be not be certified for Canada.

5. **Q: In the event a global Chinese firm was certified in Canada as above, how else could the firm benefit from this certification system?**

A. As noted, only a company headquartered globally in a contracting country or with a legal subsidiary with a substantial level of value added activity in a contracting country is eligible for the benefits. However, if Huawei had major value-added activity through a subsidiary in a contracting country, and complied with the policies, implementation rules and certification process laid out in the Principles, it would be subject to the same benefits and requirements of companies from contracting countries.

6. **Q: Assuming Great Britain is a contracting country, if Britain limits the use of Twitter during civil unrest in the name of security, would Britain be non-compliant? If Twitter adhered to the order from the British Government, would it be non-compliant?**

A: Any party to the governance of an SMO or the PCO can petition an SMO to declare that a government is not adhering to its contract to adopt policies that accord with the Principles. The SMO may conclude that such government is not acting in accord with the Principles. If the PCO (on review) approved such a decision, it would report to all contracting governments that the particular country was not acting in accord with the Principles. That "naming and shaming" would have its own effect in the court of public opinion. In addition, Twitter would then not be at risk of losing its certification by the pertinent SMO if Britain were to assert that Twitter was not following its national policies.

Twitter for its part could petition the SMO to declare that Britain was not acting in accord with the Principles, even while it continued to comply with British law. If the SMO determined that Britain was non-compliant, then Twitter would not be decertified. There is no similar avenue of redress readily available today.

7. **Q: If Bahrain limited Twitter under similar circumstances, would the answers be identical?**

A: If Bahrain is a contracting country, the same answers apply. But, if Bahrain is not a contracting country, it has no obligations and Twitter has no special recourse. The hope is that the Principles will provide sufficient incentives for membership so that countries like Bahrain would choose to become a contracting country.

8. Q: What obligations are introduced in regard to freedom of expression?

A: Governments agree in their individual contracts with the PCO that they will adopt national policies that are in accord with the Principles and the Principles embrace international conventions guaranteeing freedom of expression. No SMO can be certified by the PCO unless its charter and practices are also in accord with the Principles that are relevant to its jurisdiction.

9. Q. What can an individual that believes its human rights are violated by a company or country, or a firm that believes its property rights are being violated, do under this Implementation Plan?

A: Such a party can petition an SMO with jurisdiction over such subject matter to review its complaint. The SMO will have to set certain standing rules. However, subject to standing matters being resolved, the SMO can provide a forum that is expert, efficient, and pragmatic. Such a forum does not now exist. Moreover, if the SMO resolves a dispute in favor of a petitioner in the case of a company, the company would be decertified, and in the case of a government, the country would be subject to the "naming and shaming" discussed above.

SECTION F

Comparison Chart

Cross-Border Information Flows and Digital Trade Principles

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
	Aspen IDEA Foundation Principles						
Benefits of the Internet & Cloud Computing	• Internet and cloud computing accelerates the rate of innovation and leads to productivity gains for all nations	• Internet provides an open, decentralized platform for communication, collaboration, innovation, productivity improvement and economic growth.				• Internet an essential and irreplaceable tool for commerce; drives innovation and global economy, improves efficiency; a unique information and education resource that can help promote freedom, democracy, and human rights	These statements relate to the benefits that can be obtained through appropriate public policies for the Internet, cross-border information flows and digital trade. These benefits are why governments should take the actions and adopt the policies outlined below.
	• Internet and cloud computing expands access to markets, information and communications	• Internet allows people to give voice to their democratic aspirations, and any policy-making associated with it must promote openness and be grounded in respect for human rights and the rule of law.					
		• Strength and dynamism of the Internet depends on its ease of access to high speed networks, openness, and user confidence.				• Broadband Internet access is essential infrastructure for participation in today's economy; therefore seize emerging opportunities, such as cloud computing, social networking and citizen publications, which are driving innovation and enabling growth	

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
Public Policy Process	• Internet and cloud computing requires flexible and cooperative approaches to public policy.	• Foster voluntarily developed codes of conduct.	• Inclusion of references to voluntary cooperative efforts and voluntary codes of conduct "troubling". Concerned by references to private sector voluntary cooperative efforts to protect intellectual property rights, including "lawful steps" to address/deter infringement, which would encourage overbroad filtering, removal or blocking of content.			• Internet and its development, fostered by private sector initiatives and investments, require favorable, transparent, stable and predictable environment.	The current approach to Internet governance is working, so there is no need for significant change. The open, voluntary, multi-stakeholder process has worked well and should be maintained
		• Create multi-stakeholder policy development processes.				• Holistic approach to innovation and growth needed; requires broad engagement and guided collective action toward shared goals, such as market integration and limiting market barriers, while reducing potential frictions resulting from national approaches.	
		• Develop capacities to bring open, reliable data into the policy-making process.				• Face challenges in promoting interoperability and convergence on data protection, net neutrality, transborder data flow, ICT security, IPR.	
		• Maximize individual empowerment and responsibility.					
		• In many cases, public intervention is needed to ensure greatest practical access to these networks in our countries, particularly rural and remote areas.					
	Aspen IDEA Agenda for Action						

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
Global Approach	**Governments should embrace a global agenda for the Internet**					• Action from govs needed through national policies, but also through promotion of international cooperation. Support multistakeholder model of Internet governance: maintain flexibility and transparency. Govs have a key role to play in this model.	Public policy and regulation must recognize the global nature of the Internet.
Local Presence Requirement	• Governments should not require that facilities or information be located in a specific country or region.			• *Local Infrastructure*: Governments should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services; nor should they give priority or preferential treatment to national suppliers of ICT services in the use of local infrastructure, national spectrum or orbital resources.	• Cloud computing can reduce costs, increase security, and help the government take advantage of the latest private-sector innovations. This new industry should not be crippled by protectionist measures, so the proposal prevents states from requiring companies to build their data centers in that state, except where expressly authorized by federal law.		Requirements to locate servers or other infrastructure within a country could limit the country's ability to benefit from the global Internet and new, innovative and cost-effective services, such as cloud computing.
Intermediary Liability	• Governments should provide Cloud providers with appropriate safe harbors from liability for the content or expression of their users.	• Appropriate limitations of liability for Internet intermediaries continue to play a fundamental role w/ regard to third party content. Intermediaries can and do play an important role by addressing and deterring illegal activity. Limitations play an important role in promoting innovation and creativity, the free flow of information, and in providing incentives for cooperation between stakeholders. Within this context governments may choose to convene stakeholders in a transparent, multistakeholder process to identify appropriate circumstances under	• Internet intermediaries should not be called upon to make determinations about the legality of content passing through their networks and platforms because they are neither competent nor appropriate parties to do so. The role of intermediaries as 'mere conduits,' and accompanying liability limitations found in many OECD countries, is integral to protection of civil liberties online. Intermediaries should not be required to "assist rights holders in . . . reduc(ing) illegal content."				

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
		which Internet intermediaries could take steps to educate users, assist rights holders in ensuring their rights or reduce illegal content, while minimizing burdens on intermediaries and ensuring legal certainty for them, respecting fair process.					
Transparency & Due Process	• Any government regulation affecting data transfer and use should be transparent, equitable, necessary, provided for by law, and consistent with international standards on privacy, security, the protection of intellectual property and free expression.	• Ensure transparency, due process and accountability.		• *Transparency*: Governments should ensure that all laws, regulations, procedures and administrative rulings of general application affecting ICT and trade in ICT services are published or otherwise made available, and, to the extent practicable, are subject to public notice and comment procedures.			Transparency and due process are essential for good public policy and a critical element of a "trusted environment" that is needed to promote growth and opportunity in the digital economy.
Access to Third Party Information	• Governments should implement clear, transparent, and impartial laws, including appropriate due process protections and reasonable notice, to govern requests for third party information.						Transparency and due process are essential for good public policy and a critical element of a "trusted environment" that is needed to promote growth and opportunity in the digital economy.

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
Data Protection	• Governments should give information housed in the Cloud the same protection from government access as information stored locally or housed in any other environment.	• To ensure cost effectiveness and other efficiencies, other barriers to the location, access and use of cross-border data facilities and functions should be minimized, providing that appropriate data protection and security measures are implemented in a manner consistent with the relevant OECD Guidelines and reflecting the necessary balance among all fundamental rights, freedoms and principles.	• Concerned that text appears to endorse transborder data storage or processing without ensuring adequate levels of privacy protection and in ways that could place unjustifiable restraints on freedom of expression based on local laws.			See Trusted Environment	Data stored online should receive no less protection under the law than data stored in other ways.
Consumer Protection	• Governments should develop fast, efficient methods for gathering and sharing information regarding fraudulent and deceptive commercial practices that can victimize consumers through the Internet, and the means to deter, detect and prevent such practices.				• National Data Breach Reporting: State laws helps protect against identity theft, but are a patchwork. Legislation would simplify and standardize.	See Trusted Environment	

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
Trusted Environment	**Global Internet policy and practice must promote a functioning 'trusted environment' with respect to issues such as security, privacy, protection of intellectual property, and free expression**	• While promoting free flow of information, governments should work towards better protection of personal data, children online, consumers, intellectual property rights, and cybersecurity. Governments should also respect fundamental rights. • Limit Intermediary Liability (see relevant section) • Encourage cooperation to promote Internet security. (see Cybersecurity) • Encouraging investment and innovation requires clearly defined legal rights and a robust and fair process to protect rights, including users' rights, consistent with the need of governments to enforce applicable law. Govs, industry and civil society should work together to foster respect for the law and protect fundamental rights.	• OECD text overemphasizes protection and enforcement of intellectual property rights, even at the expense of fundamental freedoms. Text elevates cybersecurity and intellectual property rights to a level of importance comparable with internationally recognized human rights. • Concerns about qualifications within the text with respect to "lawful" content and "lawfulness."		• Legislation requires DHS to implement its cybersecurity program in accordance with privacy and civil liberties procedures developed in consultation with privacy and civil liberties experts and approved by the Attorney General. All monitoring, collection, use, retention, and sharing of information are limited to protecting against cybersecurity threats.	• IPR: recognize need for national laws and frameworks for improved enforcement. Commit to ensure action against IPR violation in digital arena, including action that addresses present/future infringements. Encourage continued innovation in legal online trade in goods and content that respects IPR. • Privacy: protection of personal data and individual privacy is essential to user trust. • Security of networks and services: is a multistakeholder issue. Pay attn to all forms of attacks against integrity of infrastructure, networks and services. Promoting user awareness is crucial. Govs have a role to play.	"Trusted environment" encompasses a very broad range of issues. Voluntary industry best practices, market-driven technology solutions and consumer education will play important roles. Governments must find an appropriate balance when considering regulations, avoiding unnecessary or counterproductive measures with unintended consequences.
Free Flow of Information	• Global Internet policy should enable open and diverse expression.	• *Promote and Protect the Global Free Flow of Information*: The Internet Economy, as well as individuals' ability to learn and express themselves, depends on the global free flow of information.		• *Cross-Border Information Flows*: Governments should not prevent service suppliers or their customers from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries.		• Arbitrary or indiscriminate censorship or restrictions on access are inconsistent with States' international obligations and unacceptable; also impede econ and social growth.	Cross-border data and information flows are essential for cross-border delivery of services, and restrictions on these flows could undermine cross-border services commitments in trade agreements and cut off trade flows. Creating a "trusted environment" could reduce a government's perceived need to block or restrict data flows.

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
		• To encourage the free flow of information online, work together to advance better global compatibility across diverse laws and regulations. While promoting free flow, governments should work towards better protection of personal data, children online, consumers, intellectual property rights, and cybersecurity. Governments should also respect fundamental rights.		• *Open Networks, Network Access and Use*: Governments should promote the ability of consumers legitimately to access and distribute information and run applications and services of their choice. Governments should not restrict the ability of suppliers to supply services over the Internet on a cross-border and technologically neutral basis, and should promote interoperability of services and technologies, where appropriate.			
Cyber Security	• All stakeholders must recognize government and private sector needs for security of the Internet.	• Implementation of internationally recognized, market-driven security standards and best practices to promote online security should be encouraged. Policies to enhance online security should not disrupt the framework conditions that enable the Internet to operate as a global open platform for innovation, economic growth and social progress.	• Concerned that OECD text elevates cybersecurity and intellectual property rights to a level of importance comparable with internationally recognized human rights.		• Penalties for Computer Criminals: Laws on cybercrime not synchronized w/ those for other crimes. Legislation clarifies, synchronizes, and sets mandatory minimums. • Provides immunity to industry, states, local gov when sharing cybersecurity information w/ DHS – with robust privacy oversight to ensure civil liberties not infringed.		The market provides a tremendous incentive to ICT hardware, software and service providers – and their users – to take the steps necessary to ensure cyber security. A cooperative public-private partnership including all stakeholders can complement market forces to enhance security. Governments must recognize the global nature of the Internet when considering cyber security policies. Global cooperation is needed. Efforts to ensure cyber security should be based on international standards and best practices.
Technology Solutions	• Internet and cloud providers and users should protect and secure information by implementing market-driven technology solutions that are updated as needed to address rapidly evolving privacy and security threats and that are appropriate for the level of sensitivity of the particular information.				• Protect Federal Government computers and networks, including management, personnel, intrusion prevention systems, data centers.		Market-driven technology solutions are an important element of a trusted and secure environment.

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
Service Provider Privacy Obligations	• Internet and cloud providers should transparently explain their information handling practices.						Service providers can go a long way towards creating a trusted environment and reducing the need for regulation by adopting appropriate, accountable and transparent information handling practices.
	• Internet and cloud providers should disclose requested third-party information only to the extent required by law and, to the extent permitted by law, should provide the affected customers with reasonable advance notice of any such compelled disclosure.	• Strengthen consistency and effectiveness in privacy protection at a global level. Privacy rules should be based on globally recognized principles, such as the OECD privacy guidelines, and governments should work to achieve global interoperability by extending mutual recognition of laws that achieve the same objectives. Privacy rules should also consider fundamental rights such as freedom of speech, freedom of the press, and an open and transparent government.					
	• Internet and cloud providers should adopt a clear, flexible and accountable framework for the flow of data.						
	Governments should encourage expansion of the Internet and the cloud.						

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
Trade	• Governments should expand the capability of the Internet to increase trade.	• *Promote an Open Internet*: The Internet's openness to new devices, applications and services is essential to its success in fostering innovation and economic growth.		• *Open Networks, Network Access and Use*: Governments should promote the ability of consumers legitimately to access and distribute information and run applications and services of their choice. Govs should not restrict the ability of suppliers to supply services over the Internet on a cross-border and technologically neutral basis, and should promote interoperability of services and technologies, where appropriate.			The Internet holds the potential to become a major "trade route of the 21st Century," bringing substantial benefits to both developed and developing countries. Cross-border data and information flows are essential for cross-border delivery of services, and restrictions on these flows could undermine cross-border services commitments in trade agreements and cut off trade flows.
Network Investment & Competition	• Governments should promote investment and expansion of the Internet as rapidly as possible.	• Promote investment and competition in high-speed broadband Internet networks.		• *Authorizations and Licenses*: Governments should authorize the provision of competitive telecom services on simple notification by a provider and should not require legal establishment. Licenses should be restricted in number only to address a limited set of issues, such as assignment of frequencies.			Access to broadband networks is a prerequisite for participation in the digital economy. Inadequate network infrastructure is a major competitive disadvantage for a country. Open competition and investment are the most effective ways to promote the deployment of broadband networks.
	• Governments should also expand the Internet by encouraging competition in broadband access and other relevant markets.			• *Foreign Ownership*: Governments should allow full foreign participation in their ICT services sectors, through establishment or other means.			
Network Regulation	• IP-based and converged services should have maximum regulatory flexibility, and be subject to regulatory obligations only to the extent they are narrowly tailored to the dynamics of this rapidly evolving sector.			• *Regulatory Authorities*: Governments should ensure that regulatory authorities that oversee ICT services are legally distinct and functionally independent from service providers, and have sufficient resources to perform their functions effectively.			Regulators should be very careful about extending traditional telecommunication regulation to the Internet and IP-based services to avoid impeding innovation. .

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
				Regulatory decisions and procedures should be impartial and publicly available.			
				• *Interconnection*: Consistent with GATS Telecom Annex, governments should ensure that public telecom service suppliers have the right and obligation to negotiate and provide interconnection on commercial terms with other providers for access to publicly available networks and services. Consistent with GATS Reference Paper, countries should ensure that public telecom service suppliers can obtain interconnection with major suppliers at cost-oriented, non-discriminatory and transparent rates.			
Spectrum Policy	• Governments should embrace the goals of (a) maximizing the availability of spectrum through continual improvements in spectrum policy, (b) technology neutrality in the design of the wireless network and its devices and (c) commercially determined approaches to the intersection of the wired and wireless segments of the Internet space.	• Promote investment and competition in high-speed broadband Internet networks.		• *Use of Spectrum*: Governments should maximize the availability and use of spectrum and should allocate spectrum in an objective, timely, transparent, and non-discriminatory manner, with the aim of fostering competition and innovation. Governments are encouraged to empower regulators with impartial, market-oriented means, including auctions, to assign terrestrial spectrum to commercial users.			Wireless broadband networks are playing an increasingly important role in innovation and economic growth. Governments should establish spectrum policies to promote competition and to enable new technologies and services.

Issue	Aspen Institute IDEA (3/16/11 draft)	OECD Principles (FINAL)	CSISAC Statement on OECD Principles (FINAL)	US-EU Trade Principles for ICT Services (4/4/11)	WH Cybersecurity Proposal (5/12/11)	G8 Deauville Declaration (5/27/11)	Comments
Technology Neutrality & Technology Choice	• Governments should promote digital product neutrality for applications and software.	• Public policies should help foster a diversity of content, platforms, applications, online services, and other user communication tools that will create demand for networks and services, as well as to allow users to fully benefit from those networks and services and to access a diversity of content, on non-discriminatory terms, including the cultural and linguistic content of their choice.		• *Open Networks, Network Access and Use*: Governments should promote the ability of consumers legitimately to access and distribute information and run applications and services of their choice. Governments should not restrict the ability of suppliers to supply services over the Internet on a cross-border and technologically neutral basis, and should promote interoperability of services and technologies, where appropriate.			Market competition is the most effective means for identifying technologies and services to meet economic and social needs. Government technology mandates can stifle innovation and create an economic handicap for the country.
	• Governments should reinforce policies that support technology neutrality.	• Internet's openness to new devices, applications and services has played an important role in its success. This stems in part from continuously evolving interaction among different groups of Internet's technical components that allows collaboration/innovation while continuing to operate independently. Maintaining technology neutrality and appropriate quality for all Internet services is also important to ensure an open and dynamic Internet environment. Provision of open Internet access services is critical for the Internet economy.	• Concerned that mention of net neutrality and common carriage are absent from OECD principles.				
Digital Literacy				• *International Cooperation*: Governments should cooperate with each other to increase the level of digital literacy globally and reduce the "digital divide".			Digital literacy is essential for a competitive workforce in today's networked global economy.