Elliott School of International Affairs
THE GEORGE WASHINGTON UNIVERSITY
Institute for International Economic Policy

MacArthur Foundation

MINERVA INITIATIVE
DEPARTMENT OF DEFENSE

Can Trade Policy Set Information Free?

Trade Agreements, Internet Governance, and Internet Freedom

Susan Ariel Aaronson,
with Miles D. Townes

KEY FINDINGS AND RECOMMENDATIONS

Finding: The Internet has empowered more people to trade information, services and goods. The Internet is both a platform for trade and a technology transforming trade, empowering more people to become market actors online.

Finding: The Internet is transforming trade policy. Policymakers in the US, EU, and Canada want to advance the free flow of information, but lack consensus on how to balance Internet openness (policies and procedures that allow netizens to make their own choices about services and content to create or share) and Internet stability (policies to prevent hacking and piracy, as well as policies to protect privacy and security).

The US is actively pushing for binding provisions in trade agreements to advance the free flow of information while challenging other nations' privacy and server location policies as trade barriers.

Many policymakers don't know how to establish a regulatory environment supportive of both Internet openness and Internet stability.

Finding: Trade policies lag trade realities, and the norms of the Internet (speed, transparency, and responsiveness) have not yet fully penetrated policymaking.

Policymakers make Internet policies in bureaucratic silos of intellectual property rights (IPR), privacy, etc... without weighing the collective effects on Internet openness or Internet freedom. Officials do not coordinate policies to promote the free flow of information with policies to advance Internet freedom.

While officials in the three case studies are responsive to their constituents, they have not figured out how to negotiate trade agreements in a way that accomodates the need for secrecy as well as meets public expectations for transparency.

Recommendation: Policymakers cannot sustain the Open Internet by relying solely on rules that advance the free flow of information. As trade agreements have long addressed governance, the US and other governments negotiating binding provisions to encourage cross-border information flows should also include language related to the regulatory context in which the Internet functions: free expression, fair use, rule of law, and due process.

The US, EU and Canada should show their commitment to Internet openness by annually reporting when and why they blocked specific applications or technologies and/or limited content (or asked intermediaries to limit access) to sites or domains. With this information, policymakers may get better understanding of how to achieve a flexible and effective balance of Internet stability and Internet openness.

(continued)

Can Trade Policy Set Information Free?

Finding: US, EU, and to a lesser extent Canadian policymakers have made expanding Internet freedom a foreign policy goal, but they have not consistently collaborated or addressed the global spillovers of national web censorship.

The US, EU, and Canada have worked internationally to develop principles to ensure an open and stable Internet, but these principles are neither universal nor enforceable. The three case studies have also agreed to principles to govern Internet trade.

Governments and netizens in the US, EU, and Canada agree that Internet openness and freedom are important goals. However, they have not clearly defined these terms or developed principles for the proper role of government in balancing Internet freedom and stability at the domestic and global levels.

Recommendation: Policymakers may need to develop shared principles for maintaining the One Global Internet and to delineate steps to take when countries do not live up to these principles. *(Do policymakers have a responsibility to protect the open Internet?)*

If preserving the One Global Internet is a top priority, the three trade giants should collaborate on capacity building and coordinate Internet policies.

Finding: Policymakers don't know if censorship is a barrier to trade. The US and EU have issued reports describing other countries' Internet policies (privacy, censorship, server location and security policies) as potential barriers to trade. None of the three governments has yet challenged Internet restrictions as a barrier to trade.

Recommendation: Trade policymakers should ask the WTO Secretariat to analyze if domestic policies that restrict information (short of exceptions for national security or public morals) are also barriers to cross-border information flows which can be challenged in a trade dispute. Moreover, policymakers should develop strategies to quantify how such policies affect trade flows.

Recommendation: WTO member states should use the trade policy review process to discuss the trade implications of member state Internet regulations that can distort trade.

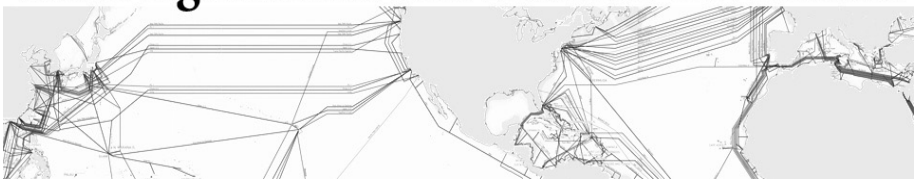
Finding: Without deliberate intent, domestic and trade policies may gradually fracture the One Global Internet.

Policymakers around the world increasingly rely on intermediaries to warn users and content creators of sites that may violate domestic laws, but this reliance on business raises questions of due process, ethics, equity, and oversight.

The three trade giants' use of bilateral/regional trade agreements with diverse Internet/e-commerce provisions may, without deliberate intent, gradually fragment the web.

Recommendation: Countries have different priorities for privacy, free speech, national security, etc...which make international harmonization of strategies to advance the open Internet unlikely. Thus, when they negotiate bilateral, regional or multilateral trade agreements, policymakers should use language to encourage interoperability among signatories' privacy, online piracy, and security policies.

Project on
Trade Agreements and Internet Governance



Can Trade Policy Set Information Free?

Trade Agreements, Internet Governance, and Internet Freedom

Susan Ariel Aaronson,
with Miles D. Townes[1]

October 2012 was an excellent month for the online marketplace eBay. The company announced that 97 percent of its commercial sellers in the US were exporting, many for the first time.[2] For eBay, the Internet is reducing distance, facilitating trust and creating one global market. However, October was a trying month for Twitter, whose users 'tweet' and read 'tweets' for stories, opinions and news. Twitter reluctantly announced that it would remove some tweets when governments asked it to do so.[3] Compared to eBay, Twitter users and executives rely on a fractured Internet with a maze of restrictions.[4]

The global Internet is creating a virtuous circle of expanding growth, opportunity, and information flows.[5] At the same time, policymakers and market actors are taking steps that undermine access to information, reduce freedom of expression and splinter the Internet.[6] Almost every country has adopted policies to protect privacy, enforce intellectual property rights, protect national security, or thwart cyber-theft, hacking, and spam. While these actions may be necessary to achieve important policy goals, these policies may distort cross-border information flows and trade. Meanwhile, US, Canadian and European firms provide much of the infrastructure as well as censor ware or blocking services to their home governments and repressive states such as Iran, Russia, and China.[7] As a result, although the Internet has become a platform for trade, trade and trade policies have served both to enhance and undermine both Internet freedom and openness.

We define **Internet freedom** as the promotion, protection and enjoyment of human rights on the Internet. We define **Internet openness** as policies and procedures that allow netizens to make their own choices about applications and services to use and which lawful content they want to access, create, or share with others. As technology, politics and culture change over time, citizens and policymakers are rethinking how to advance both freedom and openness on the web.

On one hand, advocates of Internet openness want policymakers to play a minimal role regulating the actions of networks, companies, and individuals online. They want to build on the longstanding ethos of the Internet, which defines the web as a platform separate from government and governed by net-neutrality, open standards and multi-stakeholder participation. On the other hand, policymakers must find a delicate balance between intervention and nonintervention to preserve the open Internet. *To preserve Internet freedom and openness*, they must respect freedom of information, expression, due process, and the right to privacy. To respect these human rights accruing to individuals, sometimes governments must act to maintain Internet openness; at other times, policymakers must refrain from acting. However, *to promote Internet resilience and stability*, policymakers must act in the interest of multiple stakeholders (or empower others to act) to restrict the free flow of information across borders, to enforce copyright or thwart hacking, spam, etc....

This policy brief examines how the US, the EU and Canada **use trade policies to govern the Internet at home and across borders.** The three trade giants use **trade agreements** to encourage e-commerce, reduce online barriers to trade, and to develop shared policies in a world where technology is rapidly changing and where governments compete to disseminate their regulatory approaches. Policymakers use **export controls, trade bans or targeted sanctions** to protect Internet users in other countries or to prevent officials of other countries from using Internet related technologies in ways that undermine the rights of individuals abroad. Finally, policymakers may use **trade agreements** to challenge other governments' online rules and policies as trade barriers. **We discuss how these policies, agreements, bans and strategies could affect Internet openness, Internet governance, and Internet freedom.** We do not address telecommunications or e-commerce definitional issues.

What do we mean by Internet freedom?

What is the state of Internet freedom?

- In July 2012, the United Nations Human Rights Council approved a resolution to support the "promotion, protection, and enjoyment of human rights on the Internet." The resolution A/HRC/20/L.13 affirms that people have the same rights online as they do offline, and these rights are "applicable regardless of frontiers." The resolution says states should promote and facilitate access to the Internet.

- The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank LaRue, has said governments should not block access to the Internet. He stressed that all states are obligated "to promote or to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise this right, including the Internet. Hence, States should consult with all segments of society to make the Internet widely available, accessible and affordable to all." His warning applies to how trade policies are made: they must be developed in a transparent and accountable manner.*

- However, activists and human rights officials have not achieved a clear and widely accepted definition of Internet freedom. Until recently, activists and human rights officials focused on the specific human rights that are instrumental to creating, protecting, and sharing information on the web such as the right to privacy, freedom of expression, and access to information. However, governments must provide an appropriate regulatory framework for the Internet to function in an open, efficient and responsible manner. **An appropriate regulatory framework includes government respect for due process, political participation, freedom of expression and rule of law.**

- Access to the Internet is a fundamental human right in France, Finland, and Costa Rica. Estonia and Greece stipulate that the state has legal obligations to provide access. Member states of The Council of Europe agreed that they have an obligation to provide or allow access to the Internet. (The Council of Europe promotes common and democratic principles based on the European Convention on Human Rights within 47 European countries.)

- In countries such as Brazil and India, governments provide a wide range of public services on the web including healthcare and education and hence must exert some control. These states argue that governments must actively intervene online to ensure Internet freedom.

- Although access to the Internet is greater in democracies, many democracies including India, Brazil, and the United States actively censor the web and at times abuse the privacy rights of their citizens.

- Meanwhile, officials in Iran and China (among other nations) have walled off the Internet and are essentially creating national intranets.

*See UN Human Rights Council, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank la Rue, A/HRC/17/27.

Attitudes Towards Internet Governance —
How has trade policy become a tool to regulate the Internet?

The US, the EU, and Canada share the same Internet, support the current ad hoc multi-stakeholder system, and oppose greater UN or governmental control of the web. Yet the US, EU, and Canada have fundamentally different approaches to Internet governance at the national level and in trade agreements.[8] Moreover, the three trade giants have not developed a flexible set of shared principles that do three things: encourage global information flows; ensure that regulators don't discriminate between foreign and domestic firms facilitating, creating or receiving those information flows;[9] and finally, effectively balance national and international norms for Internet openness and Internet stability.

Although the US argues that the system governing the Internet is global and diverse, US actors and norms play an outsized role on the information superhighway. US companies such as Facebook, Google, Yahoo, and Twitter dominate much of the web. Moreover, Internet governance reflects the influential role of US early web actors who wanted an ad hoc, multistakeholder, bottom up and self-regulatory approach to internet governance. However, because US (and to a lesser extent Canadian and European) companies have such huge market presence on the web, policymakers in other governments may distrust US motives. Policymakers and citizens in other countries may perceive US policymakers as acting in the interest of US companies and not in the general public interest.

Meanwhile, many other major trading nations with global clout and strong Internet presence have put forward different ideas about the role of the state online. The Chinese[10] and Russian governments[11] argue that governments must safeguard and control the Internet. For example, the Russian government now plans to use deep packet inspection to monitor the Russian Internet, which could breach citizens' privacy and free speech rights.[12] The Chinese and Russian governments have become increasingly vocal about rethinking Internet governance and have proposed greater international control over the Internet.[13] At the same time, many developing countries are just beginning to set the ground rules for the Internet in their countries.[14] Policymakers in some developing countries such as India or middle income nations such as Brazil believe that governments should do more to control the Internet.[15] Officials in these countries make the case that greater governmental control will help them provide public goods online, such as education and healthcare, and foster innovation and economic growth throughout the country.[16]

In recent years officials have developed several sets of principles to guide government action on the Internet. The Organization for Economic Cooperation and Development, OECD, a forum and think tank on global issues, has spearheaded many of these efforts and called for a holistic approach to Internet governance at the national and international level.[17] The US, EU, and Canada have worked internationally to develop principles to ensure an open and stable Internet. Some 34 nations have also agreed to principles to encourage free expression online.[18] However, these principles are neither universal nor binding. Hence, government officials have sought other venues to address cross-border Internet issues.

What International Laws Apply to the Internet?

The Internet is a decentralized network of networks, operated by several multi-stakeholder organizations such as the Internet Society, the Internet Engineering Task Force, the World Wide Web Consortium, the Regional Internet Registries and the Internet Corporation for Assigned Names and Numbers.

It is affected by international telecommunications regulations, which are made by a UN subagency, the International Telecommunication Union.

Trade rules also regulate the Internet by regulating trade in goods, information, and services.

International law applies to cyberspace. Cyber activities may in certain circumstances constitute uses of force if they create physical damage. Countries have rights to self-defense online, but responses must correspond to principles of necessity and proportionality.

International human rights law applies online, where everyone has the right to opinion and expression, and the right of access to information.

Trade agreements and policies have become an important source of rules governing cross-border information flows. First, policymakers recognize that when we travel the information superhighway, we are often trading. And Internet usage can dramatically expand trade.[19] Secondly, officials from the three trade giants understand that the Internet is not only a tool of empowerment for the world's people, but a major source of wealth for US, European, and Canadian business. Some 65-70 percent of the world's population is not yet online, so it is not surprising that these governments see a huge potential for growth in e-commerce.[20] US, European, and Canadian policymakers want to both protect their firms' competitiveness and increase market share. Finally, these officials understand that while some domestic laws can have global reach, domestic laws on copyright, piracy, and Internet security do not have global legitimacy and force. Hence, they recognize they must find common ground on internationally accepted rules governing cross-border data flows.[21] They can achieve these internationally accepted rules within bilateral, regional, or broader multilateral trade agreements.[22]

Trade agreements regulate how entities may trade and how nations may use protectionist tools. These agreements initially covered only border measures such as tariffs and quotas. Since the 1970s, however, policymakers have gradually expanded trade agreements to include domestic regulations such as health and safety regulations, competition policies, and procurement rules. So when countries block services or censor information on the Internet, policymakers from other countries may argue that these states are erecting barriers to Internet related trade. (A trade barrier is a law, regulation, policy or practice that impedes trade.) One hundred fifty-eight (158) countries rely on an international organization, the WTO, to establish rule of law on international trade.

The World Trade Organization is a set of rules defining how firms can trade and how policymakers can protect producers and consumers from injurious imports. But it is much more; it also serves as a forum for trade negotiations and settles trade disputes through a binding system. In the Internet arena, the WTO acts to promote market access, to preserve open telecommmunication networks, and to harmonize telecommunications policies that can affect international trade.[23] Although the WTO does not explicitly regulate Internet services per se, it regulates trade in the goods and services that comprise e-commerce.[24] Some seventy-four members of the WTO have agreed to implement the Information Technology Agreement. The signatories have eliminated tariffs on many of the products that make the Internet possible, such as semiconductors, set-top boxes, digital printers, and computers.[25] Since 1998, the members of the WTO have agreed not to place tariffs on data flows. But members have also disagreed on how the WTO should affect national Internet policies. The WTO's dispute settlement body has already settled two trade disputes related to Internet issues (Internet gambling and China's state trading rights on audiovisual products and services).[26] Alas, the member states have not found common ground on how to reduce new trade barriers to information flows.[27] In 2011, several nations nixed a US and EU proposal in which members would have agreed not to block Internet service providers or impede the free flow of information online.[28] Moreover, the members of the WTO have made little progress on adding new regulatory issues such as privacy and cyber security that challenge Internet policymakers.[29]

Although trade policymakers can see the benefits of trade rules as a tool to govern the Internet and encourage information flows, some individuals question whether the WTO should address Internet openness issues. First, the WTO regulates the behavior of states, not individuals or firms.[30] As a result, individuals and firms involved in online transactions have no way to directly represent their interests at the WTO. Second, information is a global public good; access to information is a basic human right under international human rights law. Hence, governments have a responsibility to ensure that their citizens have access to information through transparency mechanisms.[31] The WTO does have clear rules on transparency, due process, and political participation related to trade rulemaking.[32] But the WTO does not address human rights and has no authority to prod member states to provide an enabling regulatory context for the protection of these rights and other human rights fundamental to Internet freedom such as the right to privacy[33] or the right to free expression.[34] Third, the WTO moves slowly (as decisions are made by consensus), and thus cannot keep up with the development of new technologies. Fourth, many new online activities will require cooperative global regulation on issues that transcend market access — the traditional turf of the WTO. These issues will require policymakers to think less about ensuring that their model of regulation is adopted globally and more about achieving interoperability among different governance approaches.[35]

Because members have made little progress in trade talks at the WTO, the US, EU, and other countries have begun to use bilateral and regional free trade agreements (FTAs) to address e-commerce and other Internet issues. (These bilateral or regional agreements have many of the same problems mentioned above.)The US, EU, and Canada also use their free trade agreements to prod other governments to adopt a similar approach to regulation and enforcement. Thus, some observers see these agreements as governance agreements.[36] Table 1 summarizes how the US, EU, and Canada address Internet issues in their trade agreements.

Table 1. Case Study Free Trade Agreements: Provisions that can enhance (+) or reduce (--) Internet openness

	EU	USA	Canada
Intellectual Property Rights Provisions	Strong enforcement : +/- (Actionable provisions)	Strong enforcement : +/- (Actionable provisions)	Encourage cooperation : +/- (No binding language)
Privacy	Human/consumer right : +/- (No binding language)	Consumer right : +/- (No binding language)	Human/consumer right : +/- (No binding language)
Free Flow		Free flow : + (Proposed binding language)	Cross border data flows : + (No binding language)
Server Location		No restrictions : + (Proposed binding language)	

Free Flow of Information and Server Location —
Should trade agreements delineate clear exceptions to the free flow of information?

Free Flow and Server Location Provisions: US

The US is home to the world's largest and most influential Internet industries, and not surprisingly these companies have organized to influence trade policies and agreements. Google was the first company to argue that government restrictions on data flows and server location requirements might be a barrier to trade.[37] But Google was not the only company concerned with this issue: manufacturers and retailers also use data to cut costs, raise quality of services, and optimize energy use. In 2011, the National Foreign Trade Council, an export-oriented lobbying group with a diverse membership of multinational manufacturers, banks, and tech companies, called for provisions facilitating the free flow of information and to challenge restrictions on the flow of information as trade barriers.[38] Soon thereafter, the US Trade Representative (USTR), which negotiates trade agreements for the US, began to develop language to encourage the free flow of information as well as policies to thwart "data protectionism."

US policymakers had many reasons to be responsive to these firms. When governments restrict information flows, companies have fewer viewers and customers for their sites, content, and apps. Moreover, the US has been one of the leading advocates for Internet freedom and recognized that policies designed to facilitate the free flow of information could have spillovers for individuals. If policymakers included these provisions in trade agreements with developing countries, policymakers might gradually learn to value the open Internet. Yet US policymakers do not argue that facilitating the free flow of information will enhance Internet freedom and openness. Instead, policymakers make economic arguments; they stress that countries open to the free flow of information will grow faster, be more productive and receive more investment.[39] This strategy makes sense, as developing countries are more likely to be responsive to economic rather than human rights arguments. However, because policymakers have not linked free flow provisions to efforts to maintain Internet openness and freedom, US Internet trade policy seems incoherent and disconnected from US Internet foreign policy.

Although US trade agreements have long included language related to e-commerce,[40] the US and the Republic of Korea were the first states to include principles related to Internet openness and Internet stability in the electronic commerce chapter of the US/Korea FTA.[41] The language in this FTA was extensive. First, the two nations agreed to accept electronic signatures and included provisions designed to protect consumers online.[42] Second, the two nations agreed to encourage the free flow of information. Article 15.8 of the agreement says "the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[43] However, this provision does not forbid the use of such barriers, nor does it define necessary or unnecessary barriers. Hence the reader does not know if legitimate online exceptions to free flow such as cyber-security measures or privacy regulations are necessary or not. It is unclear if one party could use this language to challenge another party's use of such barriers. Moreover, a party could always justify using such barriers under WTO exceptions to protect national security (the Chinese argument) or to protect public morals (the Russian argument).

In 2011, the US proposed actionable language in the Trans Pacific Partnership (a regional-Asia-Pacific trade agreement being negotiated by some 11 countries) which could enhance Internet openness. Trade policymakers have not made this language public, but have asserted that the language builds on that in the US/Korea FTA.[44] The proposal supposedly includes language obligating TPP countries not to block the cross-border transfer of data over the Internet, binding obligations that countries can't require data servers to be located in the host country as a business condition, and no requirements that business enterprises must transact business through e-commerce platforms without establishing a commercial presence in the country.[45]

Officials from some of the TPP parties have not responded enthusiastically to these provisions. Some countries in the negotiation, such as Vietnam, have extensive restrictions on the Internet. Moreover, some TPP countries and individuals fear that this requirement that e-commerce platforms not be lo-

cated at home is a national security or protectionist issue.[46] Australia and New Zealand are concerned that foreign server locations could undermine their citizens' privacy rights. According to Inside US Trade, in September 2012, Australia tabled alternative language to ensure that the data-flow proposal would be consistent with its privacy laws. Australia wants TPP countries to put in place restrictions on the free flow of data, as long as the country can justify that they are not disguised barriers to trade. As of October, 2012, seven of the nine countries negotiating supposedly prefer this approach.[47] The US responded to Australian demands by proposing a more ad hoc strategy, which adheres to the Asia-Pacific Economic Cooperation Privacy Framework: firms could develop their own strategies to guard sensitive data, but each government would make this commitment enforceable through domestic institutions (such as the FTC in the US).[48] As of this writing, TPP negotiators have not yet found language that all the countries can accept.[49]

The US may be encountering significant opposition to free flow provisions because the US and some of its TPP negotiating partners have different default positions on the role of privacy, distinct approaches to regulating privacy, and attitudes regarding the free flow of information. As noted above, the US wants to ensure data can flow freely across borders with only narrow exceptions. However, Australia and New Zealand (and Canada) have made protection of privacy rather than the free flow of information a top priority for international rules governing cross border information flows. Meanwhile, countries such as Malaysia and Vietnam have not yet developed regulations to balance privacy and free flow; the US hopes that the TPP will shape these regulations and enhance the free flow of information.[50] However, these countries have yet had a domestic debate about how to balance these policy goals and may not be ready to discuss these issues internationally.

Members of Congress and activist groups are also concerned about these provisions and about TPP in general. In June 2012, some 131 members of Congress criticized USTR's strategy on the negotiations and asked for additional consultations.[51] While generally supportive of the objective of free flow, these legislators are concerned about how the US negotiates in the age of the Internet; they want a more transparent and open process. Meanwhile, some activists argue that these free flow provisions are outweighed by the copyright provisions in the TPP, which they believe unfairly punish netizens for sharing copyrighted information on the web.[52] Activists in Australia, New Zealand, Canada and Mexico are also organizing to express their concerns about the Internet provisions proposed for the TPP.[53]

Free flow provisions: Canada and the EU

Although Canada's recent FTAs speak broadly to a regulatory environment conducive to cross-border data flows, the language is not binding. Canada has included provisions on a permanent moratorium on customs duties applied to digital products delivered electronically, as well as on transparency, protection of consumers and personal information, and cooperation in the electronic commerce chapters of its previous agreements.[54] In the recently approved Colombia FTA, Canada notes the importance of "(a) clarity, transparency and predictability in their domestic regulatory frameworks in facilitating… electronic commerce; (b) encouraging self-regulation by the private sector to promote trust and confidence in electronic commerce, ensuring that… electronic commerce policy takes into account the interest of all stakeholders; and (f) protecting personal information in the on-line environment." Canada's recent FTAs also state that "each Party shall endeavor to guard against measures that unduly hinder trade conducted by electronic means." Finally, the parties agree to cooperate to maintain cross-border flows of information.[55] The EU has not included free flow of information language in its recent trade agreements.

Trade officials from both Canada and the EU say that despite their support for Internet freedom, their countries would not include **actionable** provisions regarding the free flow of information and/or server location language in trade agreements.

The US, EU, and Canada are trying to use voluntary principles to guide their work on the free flow of information and server location issues. The US and the EU are currently discussing how to address a wide range of regulatory issues that bedevil cross-Atlantic trade, in order to prepare for future FTA negotiations.[56] The EU and the US have not clarified if the future negotiations will include free flow, although it will certainly include e-commerce, services, and other sectors key to both economies. In April 2012, the US and the European Union signed a set of non-binding trade-related principles for

information and communication technology (ICT) services. The principles address commercial issues such as transparency, open networks, cross-border information flows, and the digital divide, but say nothing per se about Internet freedom or the broader regulatory context to facilitate Internet openness.[57] Meanwhile the EU and Canada have been negotiating a free trade agreement since October 2009. The negotiators will address intellectual property and cross-border trade in services, but are unlikely to discuss free flow language or Internet freedom.[58] Finally, as part of the Security and Prosperity Partnership of North America, the US, Canada, and Mexico signed "A Framework of Common Principles for Electronic Commerce" in June 2005, in which they agreed to "identify, monitor and address impediments to the free flow of information that unnecessarily impede cross-border trade or impose an unreasonable burden on the business community."[59] However, here too they made no mention of Internet freedom or the broader regulatory context that supports Internet openness.

US efforts to advance the free flow of information with language in trade agreements have met opposition from some trade partners who fear that this strategy could make it harder for their governments to protect other important goals, such as protecting privacy. Moreover, although efforts to promote the free flow of information could have positive spillovers for market actors online, US negotiators have not develop language to address the full regulatory context needed to ensure Internet openness.

Intellectual Property Rights Enforcement — *Can trade agreements protect online property rights and preserve Internet openness?*

The Internet has provided new platforms to exchange ideas, songs, news, pictures, and other information. And as the rise of Facebook, Pinterest, Weibo, and Twitter reveal, people love to share online. However, when netizens share copyrighted information online, they may violate the rights of content creators.[60]

Under US, EU, and Canadian intellectual property law, individuals can obtain limited exclusive rights to whatever economic reward the market may provide for their creations. These intellectual property rights (IPRs) provide a foundation with which intangible ideas generate tangible benefits to firms and workers. These rights are enforceable through government action and the courts. They are also enforceable through the WTO in an agreement called TRIPS.[61] This agreement helped reduce non-tariff trade barriers stemming from different IPR regimes and it also established transparency standards that require all members to publish laws, regulations and decisions on intellectual property. However, policymakers did not design copyright laws with an understanding of how people would share information online.[62] The US and EU approach to protecting IPR online is causing conflicts among high tech firms, between netizens and their governments (as shown by the ACTA debate), between firms and their customers, and in trade relations (as with the US and Canada).

IPR provisions: United States

Policymakers designed US copyright laws to protect rights holders, to encourage the creation of new knowledge, and to protect intermediaries. First, individuals can use a copyrighted work for purposes such as criticism, comment, news reporting, parody and satire, teaching, scholarship, or research according to the "fair use" doctrine created by the US Copyright Act of 1976.[63] Software developers, educational institutions, Internet search portals and others depend on 'fair use' to provide or adapt information for consumers, students, and users.[64] Several analysts have shown that these 'fair use' provisions contribute to economic growth because individuals and firms learn from and build on the work of others.[65] (Some other countries have 'fair use' including Singapore, the Philippines, Korea, Malaysia and Israel, while the UK, Canada, and Australia use the concept of 'fair dealing.'[66]) Secondly, the US recognizes that intermediaries should generally not be

held liable for copyrighted material that is posted online. Hence, the US has laws that allow rights holders to petition intermediaries to take down infringing materials. Intermediaries are supposed to comply with these takedown requests in a transparent manner that follows US norms of due process.[67]

Because Congress has made the protection of IPR online a priority for domestic law and trade negotiations, the US includes extensive language related to IPR in its trade agreements.[68] However, the IPR chapters do not always include all the attributes of US copyright laws. Moreover, other countries have different approaches to protecting IPR and judging infringement.

The US Trade Representative has developed increasingly stringent enforcement language in its trade agreements. For example, in the US/Chile FTA (which went into force in 2004), each country is supposed to develop its own procedures for notice and takedown through an open and transparent process set forth in domestic law, for effective notifications of claimed infringement, and for effective counter-notifications by those whose material is removed or disabled through mistake or misidentification. The US also prevents FTA partners from using copyright limitations and exceptions in order to allow for the retransmission of television signals over the Internet without the authorization of both the rights holder of the content and the rights holder of the signal.[69]

In recent FTAs such as Korea, the US requires its FTA partners to provide copyright terms of 70 years (20 beyond the WTO requirement), and to make it illegal for companies or individuals to circumvent protection of copyrighted work. For example, the IPR chapter in the US/Korea free trade agreement contains 35 pages of obligations which delineate 'fair use' for research and non-infringing good faith activities related to online copyright. These provisions also delineate how content holders can inform service providers of materials that are supposedly infringing, as well as a due process strategy for those who claim they were mistakenly accused of infringement. The agreement includes several side letters addressing Internet service provider obligations, copyright infringement on university campuses, enforcement against online piracy, and patent linkage. Korea also agreed to issue a policy directive establishing clear jurisdiction for effective enforcement against online piracy.[70] In its proposal for TPP, the provision requires an Internet service provider (ISP) to notify a user if it has posted infringing content and to take action against that subscriber's use of its service if the user does not take down the site.[71]

US policymakers recognize that language protecting online copyright in FTAs will not be sufficient to prevent online privacy. The US has only 19 FTAs in force and some not only contain less extensive IPR commitments, but were signed before the development of new file-sharing technologies. Hence, the US has implemented a wide range of other enforcement strategies.[72] First, a senior US official now serves as the Intellectual Property Enforcement Coordinator in the White House.[73] Her office reports on threats to US intellectual property from criminal violation.[74] Secondly, the US also conducts an annual review of its trade partners' IPR policies and practices. It creates a list of countries that don't offer "adequate and effective" protection of IPR, or "fair and equitable" market access to United States persons that rely upon intellectual property rights.[75] Thirdly, the US also lists countries and web sites as "notorious markets" in which pirated or counterfeit goods are reportedly available.[76] However, the US Congressional Research Service reports this approach is not deterring online piracy.[77] The US government and US firms have sued users and file sharing sites.[78] The US has also taken steps to move the reach of US law beyond its borders, targeting middlemen who set up web sites that share links to free access to copyright material across borders, such as Mega-upload, and charging these individuals or companies with violating the Digital Millennium Copyright Act.[79] However, legal scholars and the courts are debating whether the law has extraterritorial application.[80]

Finally, the US was a major force behind a new treaty designed to bolster enforcement of IPR online. The Anti-counterfeiting Trade Agreement (ACTA) was signed by the United States, Australia, Canada, Korea, Japan, New Zealand, Morocco, and Singapore on October 1, 2011.The negotiating countries agreed that counterfeiting has huge economic costs and can lead to consumers purchasing substandard goods. However, some activists and Internet industry representatives in the US and around the world feared that ACTA took too punitive an approach towards enforcement and by so doing, could undermine the open Internet.[81]

Although the executives of both the EU and the US accepted ACTA, the EU Parliament and the 27 EU member states have not agreed to this treaty. After street and online protests, several EU governments announced that they no longer support ACTA.[82] In late February of 2012, the European Commission announced that it was suspending consideration of the agreement and referred it to the European Court of Justice.[83] In July 2012, the European Parliament voted against ACTA. The European Economic and Social Commission, an arm of the EU summarized European concerns, "ACTA's approach is aimed at further strengthening the position of rights holders vis-à-vis the 'public'…whose fundamental rights (privacy, freedom of information, secrecy of correspondence, presumption of innocence) are becoming increasingly undermined by laws that are heavily biased in favour of content distributors… Copyright pirates are perfectly capable of eluding any form of control on the flow of data on the Internet."[84] Meanwhile, although the US Trade Representative insists Congress does not have to approve ACTA, some members of Congress disagree.[85]

In 2011, several members of Congress proposed legislation (SOPA and PIPA) to further protect copyrights on the Internet. Although the two bills were slightly different, they both required Internet service providers to shut down foreign web sites where copyrights were violated.[86] Although neither bill became law, they raised concerns in the US and abroad about extraterritoriality and due process. In conjunction with the debate over ACTA, the bills encouraged a broad public questioning about the effect of strong online copyright enforcement on the open Internet.

Meanwhile, in late 2011, Senator Ron Wyden and Representative Darrell Issa proposed a new approach, where content owners would ask the International Trade Commission to investigate whether a foreign web site profited from privacy. The foreign web site could rebut the claim to the Commission. If the Commission ruled for the copyright holder, it could direct payment firms to stop doing business with the web site; it could not shut down the site only to determine infringement. The legislators who developed this strategy also created a web site where they answer public questions on the bill and encourage citizens to mark up and improve the legislation.[87] The bill's proponents argue, "By approaching online infringement as an international trade issue, we are forced to consider not just ways to stop online infringement, but how the policies we enact impact things like cyber security, efforts to promote digital exports and international diplomacy. Moreover because norms established in the US are likely to be advanced and replicated around the world, it is important that the US carefully consider how the policies it adopts are translated and received by other countries."[88] Whatever the fate of the Wyden-Issa bill, it marks the first time that US policymakers weighed the broader regulatory context of Internet policies and how such policies might affect Internet openness.

America's current approach to protecting online copyright has many problems. First, the US demands that its trade partners focus funds and energy on enforcement, but this strategy does little to build public understanding and support for protecting copyright online. Secondly, the US strategy relies heavily on intermediaries to police the Internet for copyright violations. Although many intermediaries (whether Google, Twitter or Facebook) have a mission of facilitating Internet openness and information exchange; under this strategy these intermediaries must monitor their customers. Companies are struggling to achieve this balance. Google provides a prominent example: every six months it issues a takedown report, noting that it complies with over 90 percent of requests.[89] In May, 2012, Google said it had received 1.24 million requests

from 1,296 copyright owners for removal, targeting 24,129 domains.[90] Although the company is extremely transparent, Google does not explain how and why Google complied in one case and refused to comply in another.

Thirdly, the US approach does not consistently provide due process for individuals or firms accused of violating US copyright. Some countries use administrative or judicial procedures to decide what should be taken down and when. France and Spain have government agencies decide these issues, whereas in Chile the courts decide. The US Trade Representative has not favored this approach because it can be time consuming and may yield different results for copyright holders. For example, in the 2012 Special 301 report, USTR urged Chile to "to amend its Internet service provider liability regime to permit effective action against piracy over the Internet."[91]

The US is increasingly encountering pushback abroad towards its online copyright policies. Some critics argue that the strategy lacks transparency, accountability and an independent appeals mechanism. They are seeking legal recourse. In both Canada and France, the courts have upheld the right to download and copy music and films but did not clarify how many people can share these copies or downloads.[92] In Colombia, a US FTA partner, two Senators recently filed lawsuits against copyright revisions to Colombian law, which were adopted to bring Colombia's laws into compliance with the US/Colombia FTA. The lawsuits make the case that the Colombian law restricts the rights of Internet users to access and disclose information as well as their rights to privacy under Colombian law.[93]

IPR Provisions: EU

Like the United States, the European Union has strong and influential industries that have demanded a robust approach to protecting copyright online. But the 27 nations of the EU do not have a uniform approach to addressing this issue. Each European country makes it own decisions about when to remove content for violations of IPR.

Citizens in many European countries have become concerned about the focus on IPR enforcement and the implications of this strategy for an open Internet. In 2006, the Swedish government arrested the operators of the Pirate Bay, a file-sharing site. In response, European citizens organized both civil society groups and a political party, the Pirate Party, to rethink IPR. Pirate parties argue that the copyright system needs major reform and can't be done without addressing access, data retention, privacy and other related issues holistically.[94] Pirate Party members hold two seats in the European Parliament and several seats in state Parliaments in Germany.[95]

Given widening criticism of its approach to online IPR, the European Commission (the EC is the Executive branch of the EU) hopes to develop an updated EU-wide approach. On June 6, 2012, the European Commission kicked off an EU-wide public consultation.[96] Officials asked individuals and firms to comment on the failings of the current regime, such as notification procedures, the legal uncertainties of 27 different domestic legal regimes, and the potential for abuse where legal content is the subject of a takedown request.[97] However, the UK, Denmark, Slovenia, Belgium, Hungary and Sweden are opposed to EU-wide regulation and prefer to have a directive, which would allow common rules and maintain individual state flexibility in administering online IPR.[98]

Although member states decide their own policies for when and how to protect IPR online, the EC makes trade policy for the member states and it develops the language in trade agreements. In 2005, the EC decided that it needed a new strategy to protect IPR online. The EC aimed to reduce IPR violations in third countries, make the enforcement clauses in future bilateral or bi-regional agreements more operational, to clearly define what the EU regards as the highest international standards in

this area, and what kind of efforts it expects from its trading partners. Trade officials acknowledged that because it is difficult to detect the origin of the IPR violation and to effectively protect copyright, "EU policies should strive to improve the effectiveness and coordination of the police, the courts, the customs and the administration in general. It is also essential to ensure that the legal framework provides for deterrent sanctions."[99] Like the US, the EC is focused on enforcement, but policymakers also recognize that they must support government capacity to detect and enforce copyright violations online.

The EU began to make these changes in its Economic Partnership Agreements (EPAs — trade agreements with developing countries), such as EU-Cariforum, as well as its recent free trade agreements. The EU included rules on the liability of Internet service providers in its draft FTA between the EU and ASEAN and in EU-Korea Free Trade Agreement.[100] To meet its obligations to the EU, Korea changed its laws regarding fair use by online service providers to include acting as a conduit, caching, hosting, and information search. Korea also clarified exceptions to the prohibition against circumvention of technical protection measures online.[101]

As noted above, the EU and Canada are also negotiating an FTA. Because the agreement's provisions have not been made public or have not been leaked, we do not know if the FTA will include strong enforcement language such as that in the ATCA.[102]

IPR Provisions: Canada

Canada recently updated its copyright laws to meet the demands of new technologies.[103] Parliamentarians began this process by examining demands for takedowns and found the vast majority of copyright infringement notices are sent either by US studios (representing movies, music, and television content) or software publishers, or by agents operating on their behalf. Policymakers learned that less than two percent of notices could be attributed to Canadian copyright holders.[104] Canada ultimately changed its policy to require ISPs to warn the potential infringer that posted the material rather than requiring the ISP to take down materials (notice and notice).

Canada also has a different approach to fair use, which it calls 'fair dealing'. It allows broad exemptions for non-commercial purposes such as educa tion and parody. The Canadian courts have broadly interpreted fair dealing online.[105] The Canadian Supreme Court views teachers as well as ISPs as conduits of information.[106]

In general, Canada does not include IPR language in its free trade agreements, but rather encourages cooperation on IPR issues (see the Canada/ Colombia FTA).[107]

The Future Direction of Strategies To Enforce Online IPR

The public in the US and abroad have not generally been supportive of the US focus on enforcement. Although most web users recognize that when they breach copyright they are stealing, many web users believe that it is ethical to download music and other copyrighted/trademarked items. A recent American Assembly poll found American Internet users oppose copyright enforcement when it intrudes on personal rights and freedoms. Some 57 percent oppose blocking or filtering if those measures block legal content, although 61 percent of those polled want sites such as Facebook to reject pirated copies of music and videos.[108] At the same time, a 2012 poll commissioned by Intel of netizens in eight countries found 60 percent admit they "over share" online.[109]

Some individuals are not only concerned about the effectiveness of trade policies focused on enforcement, but about which entities do the enforcing and how that affects human rights. First, when individuals share infringing information online, they may also be sharing substantial amounts of non-infringing content. Moreover, people who download anonymously may also upload and vice versa. Internet service providers do not find it easy to figure out who posted what and who downloaded what (e.g. who is responsible). When corporate officials try to detect copyright violations in these circumstances they may, without intent, violate user rights to privacy and freedom of expression.[110] Policymakers are increasingly responsive to these concerns. For example, the UK and New Zealand are rethinking their approach to copyright on and offline.[111]

Thus, the current EU and US strategy for enforcing copyright online may without deliberate intent reduce Internet openness.

Data Protection Laws, Privacy, and Trade —
Should trade agreements regulate private information crossing borders?

In 2010, Facebook CEO Mark Zuckerberg said that "privacy is dead" because of the Internet.[112] Zuckerberg may be wrong; netizens increasingly demand that governments protect their data online. As consumers and citizens, they are both winners and losers when information is collected, processed, and analyzed across borders.[113] They benefit from cheaper and greater access to information; but their information may not be secure. As Canada's Privacy Commissioner stressed, "individuals throughout the world rely on common information and communication technologies; they share information, videos and photos using a few highly popular social networking platforms; they play online games using the same platforms and they conduct searches using the same search engines. As a result, when one of these global companies … experiences a privacy breach (as we witnessed with Sony's PlayStation Network in 2011), millions of people worldwide can be affected."[114]

Nonetheless, netizens are learning to monitor their privacy and demanding that governments protect their rights online. A 2010 survey of 5,400 adult users from 13 countries found some 84 percent of those polled are concerned about issues related to online security. Some 58 percent are concerned about being misled by inaccurate information or lies.[115] Under international human rights law, individuals have a right to privacy and to shield their information from use or misuse by others. Privacy is both a human and a consumer right. Individuals who have experienced identity fraud may find themselves with lower credit scores, stigma, stress, and discrimination. Organizations that lose personal data may experience negative publicity, distrust, and lawsuits.[116] However, barriers to trust are also barriers to access. As privacy is an issue of trust among online market actors, policymakers in the three case study countries have tried to balance protecting privacy with rules governing cross-border data flows.

The US, EU and Canada have different definitions of privacy and distinct strategies to protect it. The US sees privacy as a consumer right. The EU and Canada see privacy as both a human and consumer right.[117] The EU uses an extensive system of regulation that has broad effects on other nations' approaches to privacy. The United States uses a sectoral approach that relies on a mix of legislation regulation, and business self-regulation; recent US laws, including Sarbanes-Oxley, contain minimal guarantees of an individual's right not to have personal or confidential information exposed online.[118]

US, EU and Canadian policymakers recognize that trade is being distorted by the many different approaches to privacy. Some 100 countries have adopted regulations addressing cross-border data flows, although many major trading nations such as the US, China, India, and Brazil do not have such laws. The US Department of Commerce did a study in 2009 of business concerns around data privacy and found six challenges: 1) restrictions on transferring data between jurisdictions; 2) the lack of a recognized US privacy authority to represent the interests of US industry and citizens internationally; 3) difficulty providing a clear articulation of the US approach 4) obstacles to implementing global information management systems given conflicting foreign requirements; 5) jurisdictional ambiguity and security concerns over data held in the cloud; and 6) significant costs to track and comply with data protection laws in each country. Respondents also noted gaps in protection for consumers whose data are transferred across borders, since it is not always clear who has jurisdiction over data and what protections exist for foreign consumers.[119] Given this confusion, the OECD has tried to find common ground and interoperability among these various approaches to privacy and regulation of cross-border data flows.[120] In 1980, the members of the OECD issued the first guidelines for privacy regulations which delineated rights and responsibilities for governments, consumers, citizens, and companies transferring and processing data across borders.[121] Although the three trade giants are members of the OECD, they have favored their own approach to privacy when making trade policies. We begin with the EU system, which has become increasingly influential around the world.

Privacy: EU

The European Union has been an early leader in global efforts to advance privacy online. All 27 EU member states are also members of the Council of Europe (made of 47 European countries), and as such, they are required to secure the protection of personal data under human rights law.[122] Every EU citizen has the right to personal data protection and firms can only collect that data under specific conditions.[123] The EU also requires member states to investigate privacy violations.[124]

The European Commission's Directive on Data Protection went into effect in October 1998, and it prohibits the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection. The EU requires other countries to create independent government data protection agencies, register databases with those agencies, and in some instances, the EC must grant prior approval before personal data processing may begin. To bridge these differences in regulatory strategy, the US Department of Commerce in consultation with the European Commission developed a "safe harbor" framework.[125]

The International Spillovers of Data Protection Laws

International privacy and data protection laws have not been made interoperable. Transborder data flows involve many computers communicating on a decentralized network via a wide range of platforms including social networks, search engines, and cloud computing. *Personal data may be at risk when it travels across borders.*

Over 60 countries have adopted data protection or privacy laws that regulate the flow of information on the Internet (and other ICT platforms).

Data protection regulations and laws have:

Different objectives: Some are designed to be legally-binding human rights instruments; others such as the APEC Privacy Framework are designed to facilitate electronic commerce.

Different rationales: To prevent circumvention of national data protection and privacy laws; guarding against data processing risks in other countries; to address difficulties in asserting data protection and privacy rights abroad; and enhancing online consumer confidence.

Different legal reach: some geographically based, others extraterritorial. If data is stored in the cloud in other countries, it may be hard for individuals to exercise their rights.

Different 'default position': Some give regulators limited power to block data flows; others proceed from the assumption that personal data may not flow outside the jurisdiction unless a legal basis is present.

Different approaches to dealing with ISP: (Internet service providers) and diverse legal liability.

Result: Little regulatory efficiency or consistency. OECD suggests creating a default rule for transborder data flows, but it must incorporate human rights, trade, consumer protection, etc.

Source: Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy law: Past Present and future," OECD Digital Economy Paper, no. 187, pp. 1-18, 22, 24, 30.

The EU Directive has had an effect on trade. Because of the importance of cross-border data flows to/from the 27 EU members, some nations such as India and China are weighing how to make their laws interoperable with EU privacy provisions.[126] Meanwhile, other countries such as the Philippines have adopted EU data protection policies.[127]

Some observers of the EU approach assert that the EU focuses on process rather than outcomes or on promoting "effective good data protection practices."[128] The EC has decided to update its data protection rules to meet changes in technology and increased public concern about privacy.[129] After obtaining extensive public comment, the EU parliament is now considering a regulation developed by European Commission staff.[130] This proposed regulation includes language granting a right to be forgotten, meaning companies must delete data at the request of consumers; individuals must directly give their consent for data processing; individuals will have easier access to their own data; and companies and organizations will have to notify individuals of serious data breaches without undue delay. The EU argued these changes are necessary to "make sure that people's personal information is protected — no matter where it is sent, processed or stored — even outside the EU as may often be the case on the Internet." The EU also noted that they will help business by replacing the patchwork of national rules, lowering costs, cutting red tape and providing "assurances of strong data protection whilst operating in a single regulatory environment." To build public support, the European Commission prepared brochures to explain how these changes will affect individuals and companies as well as how these reforms will make international cooperation easier.[131]

The EC has included aspirational language on privacy in its free trade agreements. In its Economic Partnership Agreements with developing countries, Article 196 and 197 say in part: the parties recognize their "common interest in protecting fundamental rights and freedoms of natural persons, and in particular, their right to privacy, with respect to the processing of personal data."[132] In its recent free trade agreements such as EU/Korea, Chapter 6 of the agreement refers to trade in data, and Article 7.43 of the chapter on services says that each party should reaffirm its commitment to protect fundamental rights and freedom of individuals, and adopt adequate safeguards to the protection of privacy.[133]

Privacy: US

In contrast with the EU and Canada, the US does not have one broad privacy law related to data protection. Congress has passed several laws such as the Electronic Communications Privacy Act (1986), the Children's Online Protection Act (1998) and regulators have issued guidance including the Federal Trade Commission (FTC) Code of Fair Information Practices Online Report. (The Federal Trade Commission investigates and enforces many of these privacy policies.) However, these laws have major gaps; they do not require companies to get informed consent to use personal data, nor do they establish a baseline commercial data privacy framework. Congress has not been able to find common ground on new legislation. In February 2012, the White House announced "A Consumer Privacy Bill of Rights" and the Department of Commerce is convening companies, privacy advocates and other stakeholders to develop and implement enforce able privacy policies based on this proposed bill of rights.[134] The US plans to make its new approach to privacy interoperable with the privacy frameworks of its international partners.[135]

Since Congress has not written legislation on privacy in cross-border data flows, US officials have worked to accommodate the strategies of key US trade partners such as the EU. The Department of Commerce developed the US-EU Safe Harbor Framework, which permits transborder data flows to the United States for commercial purposes, with FTC enforcement as a backstop. Companies (except financial institutions and telecommunications common carriers) may apply to qualify for a safe harbor. Companies that accept the relevant voluntary, enforceable code are safeguarded so long as their practices do not deviate from the code's approved provisions (they are given a certification). However, those firms that fail to comply with the code's provisions could be subject to an enforcement action by the FTC or a State Attorney General, just as a company's failure to follow the terms of its privacy policy or other information practice commitments may lead to investigation and enforcement under current US policy.[136] The US also has a safe harbor provision with Switzerland and is a supporter of the APEC Privacy framework, which requires business to self-regulate.[137]

The US has included language related to consumer protection in FTAs, but has not mentioned privacy as an objective or included specific privacy language. As an example, in the e-commerce chapters like those for US/Panama, the agreement states that the parties recognize the importance of protecting consumers online and will cooperate on privacy.[138] The US and the EU are discussing areas for regulatory coherence before they begin negotiations on an FTA; but have only stated that "standards in the area of personal data protection should facilitate the free flow of information across borders."[139]

Privacy: Canada

Canada has developed strong national and provincial privacy protections. Canada's national privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), went into effect in 2001. The legislation established a new Privacy Commissioner who reports to the Parliament and who works to protect Canadians' privacy rights.[140] Each Canadian province also has privacy commissioners who have specific oversight responsibilities including investigation, providing guidance, promoting proactive disclosure, and educating the public.[141]

Privacy Canada has issued guidelines related to PIPEDA, noting that the legislation does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. Under the law, "a transfer for processing is a 'use' of the information; it is not a disclosure." Canadian firms are supposed to advise customers that their personal information may be sent to another jurisdiction for processing and that while the information is in another jurisdiction it may be accessed by the courts, law enforcement, and national security authorities.[142] Canadians seem increasingly reassured by these policies. According to the Privacy Commissioner's report to Parliament in 2011, public opinion surveys commissioned by the Office of the Privacy Commissioner, "the proportion of Canadians saying they feel they have less protection of their personal privacy in daily life than a decade previously has declined, from 71 percent in 2006 to 61 percent in 2011."[143]

Canada, like the EU, has not developed actionable language regarding privacy in its trade agreements. The signatories simply agree to cooperate on data privacy and consumer confidence. Article 1506: Protection of Personal Information says: "1. Each Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and 2. The Parties should exchange information and experiences regarding their domestic regimes for the protection of personal information."[144]

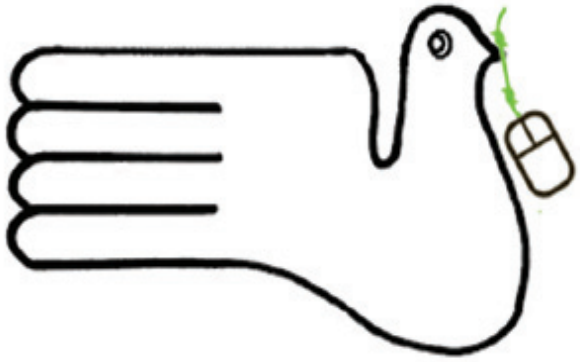
Although policymakers are beginning to address the privacy impact of data flows in trade agreements, the three trade giants have not found common ground on the trade spillovers of privacy rules. For example, some Canadian agencies have refused to send information to the US through email or data flows; they are concerned that such outsourcing could undermine Canada's security.[145] Many Canadians also believe their data can be put at risk by the U.S. government because of Patriot Act data requirements. Hence in 2004, the province of British Columbia passed legislation to restrict the disclosure of personal information outside Canada and expand the scope of personal liability and sanctions for contraventions of the BC legislation. The law required public bodies to ensure that personal information "in its custody or under its control is stored only in Canada and accessed only in Canada."[146] In 2006, Nova Scotia established similar requirements. Quebec and Alberta also established provincial laws attempting to delineate when and how personal information controlled by public bodies could be shared.[147] More recently, Canada's provincial privacy commissioners expressed concerns that a new Canada-US perimeter security action plan could undermine Canada's privacy protections.[148]
Like the EC, Canada has made privacy a priority, but in contrast with the EU it has not attempted to export its approach. However, the privacy commission recognizes that Canadian officials will need to find ways to ensure that Canada's approach to privacy is workable beyond Canada's borders.[149]

In sum, policymakers have responded to public concerns about privacy by creating domestic approaches. Taken in sum, these different approaches to privacy may or may not distort trade, but they are creating regulatory incoherence. Policymakers are trying to make these approaches interoperable. As a result, privacy rules designed to promote trust among market actors online may both distort trade and, without intent, undermine Internet openness.

Challenging Internet Regulations as Barriers to Trade —
Can trade rules be used to promote openness?

Barriers to Trade: US

As noted above, the US is not only pushing for language in trade agreements to encourage the free flow of information, but also taking steps to challenge other countries' Internet policies as barriers to trade. Thus far, the US has used naming and shaming, rather than initiate trade disputes. However, in late 2011, the US sent a letter to the Chinese government asking it to explain its Internet policies. Under paragraph 4 of Article II of the GATS, the US asked China to explain why some foreign sites were inaccessible in China, who decides when and if a foreign website should be blocked, and if China had an appeal procedure for such blockage. Although China is required to respond under GATS, the US supposedly did not receive a formal reply. The US Trade Representative is studying whether it could challenge Chinese Internet restrictions as a violation of WTO rules.[150] However, the US is unlikely to take this route, as policymakers would not want to create precedents that could limit the US or its allies' ability to restrict access to the Internet for national security reasons.[151]



BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

The US has also identified privacy rules as a barrier to the free flow of information. For example, in its most recent report on foreign trade barriers, USTR has argued that British Columbia and Nova Scotia's privacy laws discriminate against US suppliers because they require that personal information be stored and accessed only in Canada. USTR claims these laws prevent public bodies from using US services when personal information could be accessed from or stored in the United States.[152] In its 2012 report, the US also cited Australia's approach to privacy, noting Australia's unwillingness to use US companies for hosting due to concerns about privacy violations.[153] The US also complained about Japan's uneven approach to privacy and Vietnam's unclear approach.[154] Ironically, the US also argues that China's failure to enforce its privacy laws stifles e-commerce.[155]

As of November 2012, Congress is considering legislation to apply normal trade relations to Russia and Moldova.[156] The Senate Finance Committee bill contains a provision that would expand the scope of the Special 301 report, which is issued by the Office of the US Trade Representative each year, so that it also specifically includes a description of laws, policies or practices that deny "fair and equitable treatment" to US digital trade. The House bill refers to Russia alone, but the bill may not pass if it is not generalized to all US trading partners and made part of broader USG reportage of barriers to US trade.[157]

The US is also concerned that some governments have restricted information flows to the US because of the Patriot Act. USTR notes that "US companies have faced obstacles to winning contracts with EU governments and private sector customers because of public fears in the EU that any personal data held by these companies may be collected by US law enforcement agencies The United States is seeking to correct misconceptions about US law and practice and to engage with EU stakeholders on how personal data is protected in the United States."[158]

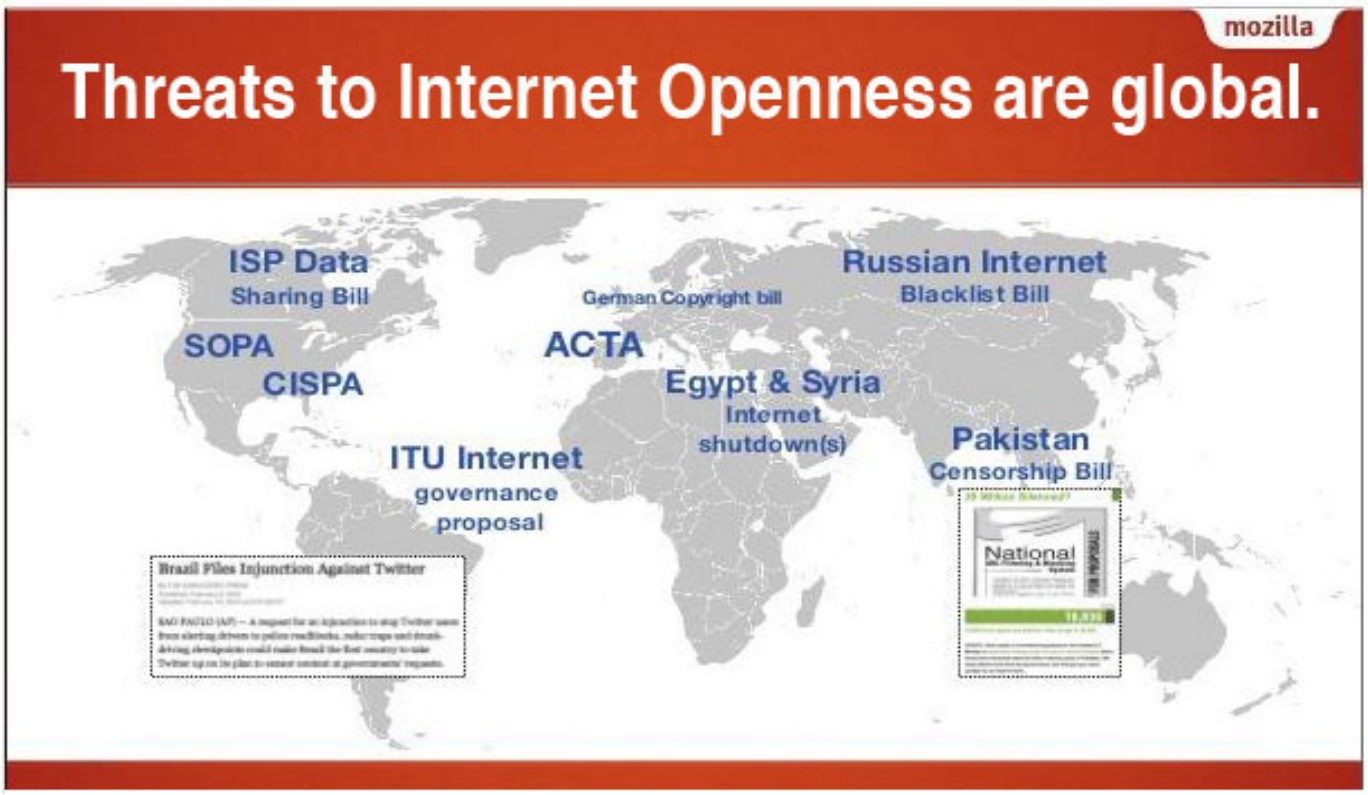
Interestingly, Antigua challenged a US barrier to information flows at the WTO. The US allows domestic online gambling, but claimed that foreign sites could

not effectively prevent fraud and money laundering. Although this objection seems reasonable, the dispute settlement body found the US was discriminating among foreign and domestic purveyors of internet gambling.[159]

Barriers to Trade: EU and Canada

In 2010, European Commission Vice President Neelie Kroes told Chinese officials that China's Internet censorship is a trade barrier that should be challenged at the WTO. However, the EC never launched a formal trade dispute.[160] The EU does not target other countries privacy policies as trade barriers, although it does view national security policies as potential barriers to trade.In addition, the EU has expressed concerns about security policies for telecom equipment in both China and India. The Indian government asked firms to provide source codes and other sensitive information in case of security breaches, which led EU officials to express privacy concerns.[161] Canadian officials have not challenged other countries' privacy policies as barriers to trade.

The US, EU, and Canada have not found common ground on when privacy, national security, and other considerations can be used to restrict the free flow of information and the location of data servers. Given these differences, policymakers need greater understanding of what domestic regulations may distort information flows and data on how these regulations affect trade (e.g. the dollar amounts of trade distortions).



Promoting Internet Freedom Abroad Through Trade —
Should policymakers use trade and other strategies to keep the Internet open?

Export Bans: US and EU

Canada, the EU and the US have often used trade policies (sanctions as well as incentives) to prevent repressive states from violating the rights of their citizens. However, the 2009 election protests in Iran and the 2011 protests in Egypt, Tunisia and other Middle Eastern states illuminated how social networking, cross-border information flows, and platforms such as Twitter could empower activists.[162] We also learned that repressive as well as democratic governments could use these platforms and web infrastructure to suppress dissent and block the free flow of information.[163]

The three case studies have considerable leverage to keep the web open. Many of these platforms, web sites, social networks, etc... as well as the hardware that makes the web possible are provided or produced by European, US, and Canadian companies. Many of the US companies are publicly listed and some European governments including France and Sweden are major investors in companies that export surveillance and communications equipment.[164] US and EU officials have sanctioned bad actors and limited access to goods or services that government officials can use to spy on or monitor their citizens' activities online. For example, the US strictly controls which nations can buy Internet filtering tools or information suppression technologies. In July 2012, the US Department of Commerce added Internet filtering tools and information suppression technologies to items under strict export controls.[165]

Unfortunately sanctions can have unanticipated consequences for the citizens that policymakers hope to assist. In 2012, the Washington Post reported that although these sanctions are supposed to make it harder for Syrian officials to spy on dissidents, they also make it harder for activists in Syria to communicate online.[166]

So far, the US and other nations have not devised a clear approach to using trade incentives or disincentives. The US Government also said that although it has a wide range of sanctions in place for Cuba, Iran, and Syria, it will grant licenses to companies that export instant messaging and other personal Internet services to those countries.[167] The US also eliminated export restrictions on "mass-market electronic products with encryption functions such as laptops and cell phones."[168]

Interestingly, the US strategy towards Internet openness and trade is being played out as the civil war rages in Syria. The Syrian government closed off the Internet for many of its citizens on November 29, yet many government sites were in fact accessible because they were hosted by US companies. According to the NY Times, the US government views such web hosting as a violation of the President's executive order on Syria, mentioned above. Ironically, the US is restricting the Internet at home in the interest of punishing the Syrian government for restricting the Internet abroad. The Department of State claimed this would promote the ability of Syrians to exercise their freedom of expression, although it is unclear how.[169] Canada and European countries also hosted some of these sites. They too must wrestle with how to protect the web abroad.

None of the three countries have developed clear guidance to their firms as to when they can sell general-use technologies to repressive states. Some technologies, such as TOR or Blackberry Instant Messenger, can be deployed for good intent (e.g. to evade governments that abuse human rights). But the same technologies can be deployed for illegal purposes (terrorism, rioting or drug trafficking). The three countries have not collaborated to develop clear standards regarding when these technologies can be sold abroad, when such sales should be monitored, and when/if they should be not be exported.

Promoting Internet Freedom: US and EU

The US, the EU, and individual EU member states are trying to develop effective strategies to help activists in repressive states access the Internet and freely express their opinions online. However, the US and EU have not developed principles regarding when and how they should act on behalf of netizens outside of the US and EU.

Policymakers acknowledge that all governments block the flow of some information for moral, ethical, privacy, cyber security or national security reasons. So officials understandably don't want to criticize the decisions of their democratically elected counterparts. Moreover, although the Internet is an obvious example of the global commons, where countries must collaborate in the broad public interest, policymakers from country A are reluctant to interfere in the affairs of country B or C, in recognition that they too would not like such interference. Thirdly, policymakers want to ensure that strategies to enhance Internet freedom abroad do not attract extensive attention and in so doing undermine rather than increase the ability of activists abroad to communicate and collaborate online.

Despite these difficulties, states are devising policies and funding innovative projects to promote Internet freedom. Sweden, the Netherlands, the EU, and the US are among the most active proponents of Internet freedom.[170] The US brings human rights activists to Geneva, Washington, and Silicon Valley to meet with fellow activists, US and international government leaders, and members of civil society and the private sector working on technology and human rights issues.[171] The US government also helped establish the Global Network Initiative, a multisectoral partnership among business, human rights groups, academics, and other interested parties. The Initiative has developed principles to guide the information technology industry on how to respect, protect and advance freedom of expression and privacy when faced with government demands for censorship and disclosure of users' personal information.[172] Yahoo, Google, Evoca, Folksam, and Microsoft, along with NGOs, churches, and academics participate in the GNI.

The EU Parliament established a €125 million fund to train and empower bloggers, online journalists and human rights defenders to circumvent censorship and evade cyber attacks.[173] The EU also set up a program, "No Disconnect" to provide citizens in non-democratic countries with tools to fight "arbitrary censorship restrictions and protect against illegitimate surveillance."[174] With EU funding, EC officials are building a "European Capability for Situational Awareness," to aggregate and visualize up-to-date intelligence about the state of the Internet across the world.[175] Meanwhile, the US has given $70 million in grants to help citizens of repressive regimes use the Internet. These grants fund technology that helps these individuals communicate securely and freely.[176] Some individuals, however, assert that these technologies are not effective because they can be easily hacked and they can be used by criminals as well as activists.[177]

Although Canada has issued several statements in support of Internet freedom, it has not made this a foreign policy priority. Despite the importance of the Internet as a platform for trade and for other sectors, none of the three trade giants uses trade capacity building per se to promote improved domestic Internet governance.

In sum, the US and the EU have adopted trade and foreign aid policies to support both Internet freedom and Internet openness. But these policies have not focused on the broader regulatory context of Internet governance at the national and international level nor built a global consensus on when it is appropriate for governments in one country to act to protect netizens in another.

Conclusion — Promoting Internet Freedom

Although the Internet is facilitating trade, trade policies serve to both enhance and undermine Internet openness. Policymakers have not achieved consensus or interoperable policies among nations which have different priorities for privacy, security, and the free flow of information. Moreover, policymakers have not figured out how to negotiate trade policies in a transparent, accountable and coherent manner supportive of the open Internet.

The US and the EU have made Internet freedom a priority. Yet neither the US nor the EU have clearly defined Internet freedom or developed a compelling and consistent argument as to why Internet freedom and openness are important to both economic growth and political stability.[178] While the US and EU have both adopted a wide range of strategies to advance Internet freedom, they have not figured out how to help governments devise an appropriate domestic regulatory context to support Internet freedom and openness. Moreover, although the three governments generally share a vision of Internet freedom, they have not collaborated to define the role of governments in supporting an open Internet or when it is appropriate to interfere in the affairs of other countries to protect netizens.

Policymakers do not make Internet related trade policies by weighing the implications of their choices for Internet openness. As a result, US and EU policies to promote cross-border information flows seem disconnected from policies to sustain the open web.

We issue these findings and recommendations in the spirit of helping policymakers in the US, EU, and Canada develop a more comprehensive, holistic, and coordinated approach.

Table 2. The struggle to balance Internet stability and Internet freedom leads to policy incoherence

Country	Policy Objective	Strategy	Implication for freedom and openness
US, EU, Canada	Advance Internet freedom.	Provide funds, technologies to ensure freedom of expression, access to Internet.	Internet freedom may be advanced. Sometimes criminals may obtain evasive technologies.
US, EU, Canada	Protect privacy as a human & consumer right.	None of the countries has pressed for a global standard but all 3 are pursuing interoperability.	Have not clarified when privacy rules act as a barrier to trade. Have not developed common ground on privacy as human or consumer right.
US, EU, Canada	Protect national/cyber security	Monitor and occasionally restrict access.	Have not clarified when policymakers can block access to information to support national security.
US	Challenge privacy regulations as a barrier to trade	List in trade barrier report.	Send message protecting privacy should be subordinated to encouraging information flows.
US	Challenge concerns about server location/cloud computing as a barrier to trade	List in trade barrier report.	Have not clarified if server requirements distort trade. Have not found national or international balance between privacy, server location, and national security.
US, EU	Establish regulatory model and protect online IPR.	Insist that FTA partners adopt copyright protection model, focus on enforcement. Rely on intermediaries to enforce.	Put intermediaries in difficult position of reducing access to information, only some of which may violate copyright.
US	Use trade agreements to facilitate the free flow of information among nations.	Does not include provisions in FTAs that address whole of regulatory governance to support open Internet. Requires nations to include these provisions before achieving domestic consensus on Internet governance.	Unable to effectively promote Internet openness. Do not focus on broad vision of regulatory environment necessary to support open Internet. Have not found shared approach to fostering free flow, server location, privacy, etc.
US, EU, Canada	Establish precedent and treaty to protect online copyright (ATCA).	Get major markets to sign on.	Send message free expression and access to information less important than protecting IPR. Focus on enforcement, but little effort to promote netizen understanding that online piracy is theft.

Endnotes

1. We are very grateful to our funders at the MacArthur, Boell, and another anonymous foundation. We also want to thank the many individuals who helped us in our research in the US, EU, and Canada. Several individuals went out of their way to review this draft and provided helpful comments: they include Usman Ahmed, Mark MacCarthy, Hosuk Lee Makiyama, Daniel O' Connor, Amy Porges, and Ben Scott. Any mistakes herein are our own.

2. eBay also reported that 81% of its sellers sell to multiple markets. Sidley Austin, LLP for eBay, "Enabling Traders to Enter and Grow on the Global State," 2012, 4, 14, at . http://www.ebaymainstreet.com/news-events/new-ebay-roadmap-highlights-economic-opportunities-commerce-30-europe. George R. G. Clarke and Scott J. Wallsten, "Has the Internet Increased Trade? Developed and Developing Country Evidence," Economic Inquiry 44, no. 3, (7/2006, 465-484 and H. Hauser and S. Winch-Vincent "A Call for a WTO E-Commerce Initiative," International Journal of Communications Law and Policy, 6, 2000, p. 2, fns. 2-4.

3. Steven Erlanger and Alan Cowell, "Twitter Removes Anti-Semitic Postings, French Jewish Group Says," New York Times, 10/19/2012, http://www.nytimes.com/2012/10/20/world/europe/british-police-investigate-twitter-account.html?_r=0. Twitter said it complied with German government requests to remove posts from a neo-Nazi group, and the company also took down anti-Semitic posts in France. Four Bahraini Twitter users were arrested, and a Turkish composer was also forced to defend his tweets in court. "Turkish Pianist on Trial for Insulting Islam," Associated Press, 10/18/2012, http://www.google.com/hostednews/ap/article/ALeqM5gzMP0_IW4ylj-ujU4FS1rsCoEXew?docId=ef9c5bc45136468b8a8f089a514376a3; and Global Voice, "Four Tweets Arrested in Bahrain," http://advocacy.globalvoicesonline.org/2012/10/17/four-tweeps-arrested-in-bahrain/

4. Twitter, "Country Withheld Content," https://support.twitter.com/articles/20169222-country-withheld-content#, Alex Macgillivray, the chief counsel of Twitter wrote, "We have found that transparency is vital to freedom of expression. Upon receipt of requests to withhold content, we will promptly notify affected users unless we believe we are legally prohibited from doing so (for example, if we receive an order under seal). We also clearly indicate within the product when content has been withheld. …We strongly believe that the open and free exchange of information has a positive global impact, and that the Tweets must continue to flow."

5. Lendle, Andreas; Olarreaga, Marcelo; Schropp, Simon; and Vezina, Pierre-Louis; "There goes gravity : how eBay reduces trade costs, World Bank Policy Research Paper," No. 6253, 10/2012, http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2012/10/25/000158349_20121025161729/Rendered/PDF/wps6253.pdf

6. David Kurt Herold, "An Inter-Nation-al Internet: China's Contribution to Global Internet governance? September 5, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1922725. He argues that the world now has 192 *distinct, albeit connected Intranets*.

7. http://opennet.net/blog/2011/03/oni-releases-2010-year-review; and http://opennet.net/about-filtering . Also see http://www.washingtonpost.com/world/national-security/syria-using-american-software-to-censor-Internet-experts-say/2011/10/22/gIQA5mPr7L_story.html; and http://www.fastcompany.com/1743849/how-american-companies-help-middle-eastern-governments-censor-the-Internet

8. The US approach to governance differs from that in the EU and Canada. European states generally have a history of corporatism where business, government and labor work cooperatively, which is evident in the EC's approach to rethinking privacy and IPR provisions. Canada is somewhere in between the US and the EU model. Canadians see government as more of an enabler and partner, and Canadian policymakers tend to govern from the center. On Europe, Remarks of Marietje Schaake, 11/2/2012, at Congressional Internet Caucus Advisory Committee. Schaake is a member of the Committee on Foreign Affairs, EU Parliament. On Canada, see Crossing boundaries, Canada 2020 Working Group, Progressive Governance for Canadians: What you need to know, 2012, p. 23. http://www.canada2020.ca/files/Canada_2020_CB_Book.pdf

9. Rohan Samarajiva and Hosuk Lee-Makiyama, "Whither Global Rules for the Internet? The Implications of the world Conference on International Telecommunication (WCIT) for International Trade," ECIPE Policy Brief, No. 12, 2012, p. 3 http://www.ecipe.org/publications/wcit/

10. Information Office of the State Council of the People's Republic of China, "White Paper on the Internet," 6/8/2010, http://www.china.org.cn/government/whitepaper/node_7093508.htm

11. Beginning November 1, 2012, the Russian agency *Roskomnadzor* (the Agency for the Supervision of Information Technology, Communications and Mass Media) compiles lists of web sites to be blocked and instructs Internet service providers (ISPs) to block access. Host providers must also ensure they are not in breach of current law by checking their content against the database of outlawed sites and URLs published in a special password-protected online version of the Register open only to webhosters and ISPs. Federal law of Russian Federation no. 139-FZ of 2012-07-28, http://en.wikipedia.org/wiki/Federal_law_of_Russian_Federation_no._139-FZ_of_2012-07-28

12. Andrei Soldatov and Irina Borogan," The Kremlin's New Internet Surveillance Plan Goes Live Today," Wired, 11/1/2012, http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/

13. On Russian and Chinese Views, Information Security Doctrine of the Russian Federation, Approved by V. Putin, 9/9/2000, http://www.mid.ru/bdomp/ns-sndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument; Timothy. L Thomas, "Information Security Thinking,: A Comparison of US Russian and Chinese concepts,", July, 2001, http://fmso.leavenworth.army.mil/ts/infosecu.htm; . On the proposals to rethink Internet governance at the ITU, see Grant Gross, "US Tech Leaders Fear Proposed Internet Regulations, Taxes at ITU Meeting," CNET, 5/12/2012, http://www.pcworld.com/article/256596/us_tech_leaders_fear_proposed_Internet_regulations_taxes_at_itu_meeting.html and Eric Pfanner, "Debunking Rumors of an Internet Takeover," NY Times, 6/11/2012, http://www.nytimes.com/2012/06/11/technology/debunking-rumors-of-an-Internet-takeover.html?pagewanted=all

14. Scott J. Wallsten. "Regulation and Internet Use in Developing Countries" Economic Development and Cultural Change 53. #2 (2005): 501-523.

15. As example, India proposed a new UN Committee on Internet Related Policy (CIRP) at the 66th General Assembly on Oct 26, 2011. Recently under pressure, India has backed away from proposals advocating greater government control of the Internet. Sandeep Bamzai,"Muzzlers of the Free Internet: India is lobbying for bureaucrats to run the worldwide web," Daily Mail, 10/20/2012, http://www.dailymail.co.uk/indiahome/indianews/article-2220692/How-India-helped-bunch-bureaucrats-custodians-Internet.html;

16. Scott Wallsten,"Regulation and Internet Use in Developing countries," World Bank Policy Research Working Paper No. 2979, 12/2002, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=366100 , p. 7; Ministry of Foreign Affairs of the Netherlands, "Background Paper,: The Role of Governments in Protecting and Furthering Internet Freedom," 2011, http://www.minbuza.nl/binaries/content/assets/minbuza/en/the_ministry/the-role-of-governments-in-protecting-Internet-freedom---freedom-online.pdf; and UN General Assembly Conference Secretariat, "The Digital Economy: Integrating the LDCs Into the Digital Economy," A/Conf.19/L.15, 19 May 2001 and Internet Governance Forum, TS Workshop 182: Global Internet Related Public Policies: Is there an Institutional Gap? 9/2011, http://www.intgovforum.org/cms/component/content/article/71-transcripts-/919-ts-workshop-182-global-Internet-related-public-policies-is-there-an-institutional-gap

17. OECD, "The Role of Internet Intermediaries in Advancing Public Policy Objectives: Forging Partnerships for Advancing Policy Objectives for the Internet Economy, Part II, DSTI/ICCP/(2010)11/Final, 26/22/2011, p. 32-33, http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=DSTI/ICCP%282010%2911/FINAL&docLanguage=En

18. In June 2011, the thirty eight members of the OECD and Egypt agreed to the OECD Principles for Internet Policymaking. They agreed to promote and protect free flow of information, to limit Internet intermediary liability; strengthen individual empowerment online, among other goals. http://www.oecd.org/Internet/innovation/48289796.pdf . The Dutch government organized a meeting in 2011 for governments to stand up for free expression on the Internet. Some 17 governments have now agreed to join the Freedom Online Coalition. They include many members of the EU (but not the European Commission), Canada and the U.S. as well as developing countries, Ghana, Kenya, the Maldives, and Mongolia.. The signatories agreed to share information about censorship; to collaborate to support free expression, to promote business responsibility re. the Internet and human rights; and promote Internet freedom. See http://www.government.nl/news/2011/12/14/coalition-of-countries-for-free-Internet.html; and http://www.freedomonlinekenya.org/home

19. In a study of 27 developed and six six developing countries Clarke and Wallsten found a 1 % point increase in the number of Internet users correlates with a boost in exports of 4.3 percentage points. George R. Clarke and Scott J. Wallsten,"Has the Internet Increased Trade? Developed and Developing Country Evidence," Economic Inquiry, 44, no. 3 (2006): 456-484.

20. "OECD Policy Brief: The Future of the Internet Economy," June 2008, 1, 2, at http://www.oecd.org/dataoecd/20/41/40789235.pdf; Internet World Stats, http://www.internetworldstats.com/stats.htm, last viewed 11/27/2012.

21. Several scholars recognized that Internet restrictions could be trade barriers and that the world would need to develop shared rules for information flows. See Tim Wu, "The World Trade Law of Censorship and Internet Filtering," http://papers.ssrn.com/sol3/papers.cfm?abstract_id=882459; and Brian Hindley and Hosuk Lee-Makiyama, "Protectionism Online: Internet Censorship and International Trade Law", Dec. 2009. http://www.ecipe.org/media/publication_pdfs/protectionism-online-Internet-censorship-and-international-trade-law.pdf

22. Karen Coppock and Colin Maclay, "Regional Electronic Commerce Initiatives: Findings from three case studies on the Development of regional electronic commerce initiatives," Information Technologies Group, Harvard University, 7/2002, http://cyber.law.harvard.edu/itg/libpubs/andes pubs/Regional_Ecommerce.pdf

23. The WTO was built on the international trade agreement GATT, which had governed trade since 1948. Since 1998, Members have agreed not to put duties on e-commerce. See The Geneva Ministerial Declaration on Global Electronic Commerce, WT/MIN (98/DEC/2, 25 May, 1998. Also see Doha Ministerial Declaration, Nov. 14, 2001, par. 34, http://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_e.htm#electronic and http://www.wto.org/english/thewto_e/whatis_e/tif_e/bey4_e.htm. The WTO had an Internet tax moratorium from 1999-approximately 2001. http://www.tax-news.com/news/WTO_Ministers_Extend_Internet_Tax_Ban_For_2_Years____183.html

24. Sacha Wunsch-Vincent, "WTO, E-Commerce and Information Technologies, From the Uruguay Round through the Doha Development Agenda: A Report for the UN IDT Task Force", Markle Foundation, 2005. http://www.iie.com/publications/papers/wunsch1104.pdf

25. These zero tariffs are extended to all World Trade Organization members on a most-favored nation basis. NA, "Norway, Thailand Join Small-Group Discussions To Expand ITA," Inside US Trade, 7/20/2012, http://insidetrade.com/Inside-US-Trade/Inside-US-Trade-07/20/2012/norway-thailand-join-small-group-discussions-to-expand-ita/menu-id-172.html See The Geneva Ministerial Declaration on Global Electronic Commerce, WT/MIN (98/DEC/2, 25 May, 1998. Also see Doha Ministerial Declaration, Nov. 14, 2001, par. 34, http://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_e.htm#electronic

26. "United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services", http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm; and "China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products", http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds363_e.htm

27. WTO, "15 Years of the Information Technology Agreement: Trade, Innovation and Global Production Networks," p. 35: and WTO, "News on Information Technology Agreement, 11/1/2012, http://www.wto.org/english/news_e/news12_e/ita_01nov12_e.htm . However, discussions on free flow may be revived as part of a plurilateral agreement on the liberalization of services. See "WTO Members Seek Services Accord as Doha Stalls, US Says," Bloomberg News, 3/2/2012; and "US steps up push for WTO services trade talks," Reuters, 3/2/2012. 2012.http://www.ecipe.org/media/media_hit_pdfs/ecipe-esf-seminar-in-brussels.pdf

28. The WTO's General Agreement on Trade in Services (GATS) sets limits as to when governments could block services (such as Internet services), but it is vague: Members can only invoke this exception to the rule "where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society." General Agreement on Trade in Services (1994) 33 ILM, 1167, Article XIV, n. 5. On US and EU proposal forbidding blocking, see US Tables Second Part of TPP Data Proposal, But Talks Still Preliminary," Inside US Trade, 11/10/2011.

29. Data protection regulations are exempted from scrutiny under the GATS as long as these regulations are not a disguised restriction on trade.

30. However, some of the WTO's disciplines directly affect commercial conduct, as example, delineating a telephone company's obligation to treat customers in a non-discriminatory manner. I am grateful to USTR staff for that insight.

31. In fact, in the first session of the UN General Assembly member states agreed, "Freedom of information is a fundamental human right and ... the touchstone of all the freedoms to which the United Nations is consecrated. Inge Kaul, Isabelle Grunberg and Marc A. Stern, eds., Global Public Goods: International Cooperation in the 21st century (NY, Oxford University Press, 1999), http://web.undp.org/globalpublicgoods/Executive_Summary/executive_summary.html#introduction; Keith E. Maskus and Jerome H. Reichman, eds. International Public Goods and Transfer of Technology Under a Globalized Intellectual Property Regime, Cambridge, UK: Cambridge University Press, 2005; and Toby Mendel, "Freedom of Information as an Internationally Protected Human Right," http://www.article19.org/data/files/pdfs/publications/foi-as-an-international-right.pdf.

32. See Susan Ariel Aaronson and M. Rodwan Abouharb, "Unexpected Bedfellows: The GATT, the WTO and Some Democratic Rights," June, 2011, International Studies Quarterly 55:2, pp. 379-408.

33. The WTO Services Agreement addresses protection of privacy as an exception, XIV (c) (ii)]. WTO)GATS at http://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm; the WTO telecom agreement [5 (d)]WTO) also says "a Member may take such measures as are necessary to ensure the security and confidentiality of messages, subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade in services." See Telecom Annex at http://www.wto.org/english/tratop_e/serv_e/12-tel_e.htm

34. On the WTO and human rights see, Susan Ariel Aaronson and Jamie Zimmerman, Trade Imbalance: The Struggle to Weigh Human Rights Concerns in Trade Policymaking (Cambridge; 2007), pp. 3-4, 18-19; and for a literature review, Monash Law School, "WTO and Human Rights Literature Review", 9/2005, see http://www.law.monash.edu.au/castan-centre/projects/wto/wto-lit-review-05.pdf.

35. For an excellent overview, see Mira Burri and Thomas Cottier, eds., Trade Governance in the Digital Age (for the World Trade Forum) (New York, Cambridge U. Press), 2012.

36. Simon Evenett and Michael Meier, "An Interim Assessment of the US Trade Policy of Competitive Liberalization," World Economy, 2008, 31 (1): 31-66; and Jean-Pierre Chauffour and Jean-Christophe Maur, Preferential Trade Agreement Policies for Development: A Handbook (World Bank, 2011), pp. 17-35.

37. Google, "Enabling Trade in the Era of Information Technologies: Breaking down Barriers to the Free Flow of Information," 11/15/2010; and Google letter to Don Eiss, Trade Policy Staff Committee, re. Request for Public Comments to Compile the National Trade Estimate Report on Foreign Trade Barriers, Docket No. USTR-2011-0008.

38. NFTC, Promoting Cross-Border Data Flows: Priorities for the Business Community, 2011,http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf

39. Gary Locke, Secretary of Commerce, "Remarks at U.S. Chamber of Commerce on Global Flow of Information on the Internet," 6/16/2011, http://www.ntia.doc.gov/speech-testimony/2011/remarks-us-chamber-commerce-global-flow-information-internet

40. For a good overview of the earlier language see Brian Bieron and Usman Ahmed, "Regulating E-commerce Through International Policy: Understanding the Trade law Issues of e-commerce," Journal of World Trade, 46:3 (2012):548-555. Bieron and Ahmed argue that earlier FTAs included binding language related to MFN for digital products, no customs duties on digital goods, cooperation, transparency in governance, and aspirational language for consumer protection.

41. As with earlier US FTAs, the parties agreed not to impose duties fees or other charges related to e-commerce., to provide national treatment and MFN to e-commerce etc…The agreement went into force in 2012.

42. US International Trade Commission, "Potential Economy Wide and Selected Sectoral Effects of the US-Korea Free Trade Agreement," Investigation No. TA-2104-24, Publication 3949, September 2007, pp. 4-5 fn. 98, http://www.usitc.gov/publications/pub3949.pdf

43. US/Korea FTA, Chapter 15, Article 15.8 "Electronic Commerce", http://www.ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text

44. Knowledge Ecology International to Senator Patrick Leahy, 1/26/2012, http://keionline.org/node/1349

45. NA, "TPP Countries to Discuss Australian Alternative to Data-Flow Proposal," Inside US Trade,

46. Remarks of Rob Atkinson, "Cloud Computing for Business and Society", Brookings Institution, Washington DC, Jan 20, 2010, http://www.brookings.edu/~/media/events/2010/1/20 cloud computing/20100120_cloud_computing.pdf. Also see Paul Taylor, "Privacy Concerns Slow cloud Adoption," Financial Times 8/2/2011, http://www.ft.com/intl/cms/s/0/c970e6ee-bc7e-11e0-adac-00144feabdc0.html; and Jennifer Baker, "EU upset by Microsoft warning on US access to EU cloud," Computerworld, http://www.computerworld.com/s/article/9218167/EU_upset_by_Microsoft_warning_on_US_access_to_EU_cloud/

47. NA, "US, Australia make Little Headway Toward Resolving differences on Data Flows," Inside US Trade 9/12/2012.

48. *Ibid*.

49. NA, "Key Areas of TPP Talks at Different Stages After 30 Months of Effort," Inside US Trade 9/5/2012; NA, "TPP Countries to Discuss Australian Alternative to Data-Flow Proposal," Inside US Trade 7/5/2012; and NA, "USTR Identifies Three Priority Areas For TPP Services Chapter", Inside US Trade, 10/25/2012.

50. NA, "USTR official: US Still Faces Big challenges on TPP Data Flow Proposal," Inside US Trade, 9/24/2012.

51. NA,"131 House Dems Criticize Direction Of TPP; Demand Greater Transparency," Inside US Trade 6/29/2012, and Author observations at event sponsored by this project, Can "Can Trade Agreements Facilitate the Free Flow of Information? The Trans-Pacific Partnership as a Case Study," Elliott School of International Affairs, Washington, DC, 9/21/2012, http://www.gwu.edu/~iiep/events/tradeandinformation_tpp.cfm

52. NA, "Academics Describe US Clarifications in TPP Copyright Proposal," Inside US Trade, 9/14/2012; and Author observations at event sponsored by this project, Can "Can Trade Agreements Facilitate the Free Flow of Information? The Trans-Pacific Partnership as a Case Study," Elliott School of International Affairs, Washington, DC, 9/21/2012, http://www.gwu.edu/~iiep/events/tradeandinformation_tpp.cfm

53. NA, "After 30 Months of Negotiations, TPP Talks still have a long way to Go," Inside US Trade, 9/4/2012; NA, "Wyden, Issa Join Forces in Latest Effort for More Transparency in TPP," Inside US Trade, 9/6/2012; NA, "Academics Describe US Clarifications of Key Provisions in TPP Copyright Proposal," Inside US Trade, 9/12/2012.

54. Government of Canada, "Report of the Joint Study on the Possibility of a Canada-Japan Economic Partnership Agreement", 3/7/2012, / http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/japan-japon/study-report_rapport-etude.aspx?lang=eng&view=d#19; and Canada/Jordan FTA, "E-commerce provisions", http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/jordan-jordanie/chapter3-chapitre3.aspx?lang=eng&view=d

55. Canada-Colombia Free Trade Agreement, Chapter Fifteen, "Electronic Commerce", http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/colombia-colombie/chapter15-chapitre15.aspx?view=d

56. NA, "Dreier Sees Less Enthusiasm In Congress For Outreach To EU Than TPP," Inside US Trade, 8/24/2012; NA, "US, EU Seek To Tackle Trade Barriers In Advance Of HLWG Final Report", Inside US Trade, 10/19/2012

57. European Union-United States Trade Principles for Information and Communication Technology Service, 4/2012, http://www.ustr.gov/webfm_send/2780

58. EC, "International Affairs: Free Trade Agreements", http://ec.europa.eu/enterprise/policies/international/facilitating-trade/free-trade/index_en.htm#h2-2; and Canada, DFAIT, "Consultations towards a Canada-European Union comprehensive economic agreement," http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/eu-ue/cepa-consult-apeg.aspx?lang=eng&view=d

59. Statement on the Free Flow of Information and Trade in North America, June 2005 http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00515.html

60. Executive Office of the President, 2011 U.S. Intellectual Property Enforcement Coordinator, "Annual Report on Intellectual Property Enforcement, 3/2012, 10-11.

61. The TRIPS agreement covers how nations should give adequate protection to intellectual property rights; how countries should enforce those rights; how to settle disputes on intellectual property between members of the WTO; and special transitional arrangements during the period when the new system is being introduced The TRIPS agreement took effect on 1 January 1995, developed countries were given one year to ensure that their laws and practices conform with the TRIPS agreement. Developing countries and (under certain conditions) transition economies were given five years, until 2000. Least-developed countries have 11 years, until 2006 — now extended to 2016 for pharmaceutical patents. Proponents of the TRIPS agreement argued that it would create a framework which encourages domestic innovation, and by protecting foreign IPR holders, gave them incentives to invest in production and research in the developing world. http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm,

62. Google, (UK) "Submission to the Independent Review of Intellectual Property and Growth, 3/2011, p. 3, 3.5,

63. The US Copyright Act is 17 USC.§ 107. Much of the Internet industry grew under in the US under fair use.

64. Thomas Rogers & Andrew Szamosszegi, "Fair Use in the US Economy: Economic Contribution of Industries Relying on Fair Use," CCIA, 2010), pp. 11-12, available online at http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000354/fair-use-study-final.pdf

65. *Ibid*, and Jared Huber and Brian T. Yeh, "Copyright Licensing in Music Distribution, Reproduction, and Public Performance", CRS Report RL33631, 8/20/2006.

66. Brian Bieron and Usman Ahmed, "Regulating E-commerce Through International Policy: Understanding the Trade law Issues of e-commerce," Journal of World Trade, 46:3 (2012), p. 563.

67. The Digital Millennium Copyright Act is P. L. 105-304.

68. The Congress called on the executive to work to extend IPR protection to new and emerging technologies and to new methods of transmission and dissemination. Congress also wanted to bring other governments IPR in line with US law (or to put it differently to extend US regulation to other markets). 2002 Bipartisan Trade Promotion Authority Act, P.L. 107-210, Sec. 2102(b)(4).

69. U. S. Chile FTA, Article 17.11, p. 17-27 through 17-30), http://www.ustr.gov/sites/default/files/uploads/agreements/fta/chile/asset_upload_file912_4011.pdf

70. Letters from Hyun Chong Kim and Susan C. Schwab, 6/20/2007, http://www.ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file948_12737.pdf and http://www.ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file948_12737.pdf; Us/Korea FTA, Article 18.5. and Article 18.7 at http://www.ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file273_12717.pdf

71. NA, "In Shadow Of ACTA, EU Drops Criminal IPR Provisions In CETA Talks," Inside US Trade, 11/2/2012.

72. US industries such as software, music, films, and computer fames rely on IPR protection. They lose billions of dollars in revenue from due to piracy and counterfeiting.

73. The US also has a portal on its IPR policies and enforcement. www.iprcenter.gov

74. National Intellectual Property Rights Coordination Center, "Intellectual Property Rights violations: A Report on Threats to United States Interests at Home and Abroad," http://www.iprcenter.gov/reports/ipr-center-reports/IPR Center Threat Report and Survey.pdf/view

75. The Omnibus Trade and Competitiveness Act P. L. 100-418 included the Special 301 provisions.

76. USTR, "Out of Cycle Review of Notorious Markets,"2/28/2011, http://www.ustr.gov/webfm_send/2595

77. Shayerah Ilias and Ian F. Fergusson, "Intellectual Property Rights and International Trade, CRS Report, RL34292, 2/17/2011, p. 12, also see 31-32, http://www.ieeeusa.org/policy/eyeonwashington/2011/documents/iprtradeagreements.pdf

78. Torrent Freak, "First Software Maker Joins Bit-Torrent Lawsuit Bonanza,"11/16/2012, http://torrentfreak.com/first-software-maker-joins-bittorrent-lawsuit-bonanza-121116/

79. Somini Sengupta, "US Pursuing a Middleman in Web Piracy," NY Times, 7/12/2012, http://www.nytimes.com/2012/07/13/technology/us-pursues-richard-odwyer-as-intermediary-in-online-piracy.html. The sites associated with Megaupload were shut down by the United States Department of Justice 1/19/2012. BBC News, "Megaupload extradition case delayed until March 2013," http://www.bbc.co.uk/news/technology-18779866

80. Benjamin A. Neil and Richard W. Winelander " An examination of jurisdictional defenses available to foreign defendants to copyright claims brought in U.S. courts," Journal of International Business and Cultural Studies, http://www.aabri.com/manuscripts/09334.pdf and Adam D. Fuller, "Extraterritorial Implications of the Digital Millennium Copyright Act;". 5 Case W. Res. J. Int'l L. 89 (2003)

81. On IPR as a customs problem see WTO News, "Intellectual Property: Formal Council Meeting: Council debates how and Where to handle counterfeit trademarked goods," 6/5/2012, http://www.wto.org/english/news_e/news12_e/trip_05jun12_e.htm; and on concerns about ATCA, http://www.ifla.org/en/news/ifla-raises-concerns-about-acta; and http://www.publicknowledge.org/issues/acta; and http://www.euroispa.org/news/63-Internet-industry-concerns-on-the-anti-counterfeiting-trade-agreement

82. Monika Ermert, “Most EU Members Sign ACTA; SOPA-Style Protests Building,” 1/27/2012, Intellectual Property Watch http://www.ip-watch.org/2012/01/27/most-eu-members-sign-acta-sopa-style-protests-building/?utm_source=weekly&utm_medium=email&utm_campaign=alerts; Over 1.75 million people have signed a petition on avaaz.org urging EU Members not to ratify ACTA. Infojustice.org, “Resistance to ACTA in Europe Grows,”2/8/2012, http://infojustice.org/archives/7886.

83. RT News, “EU Suspends Consideration of ACTA, Refers Treaty to Court,” 2/21/2012, http://rt.com/news/eu-suspends-acta-ratification-955/ and EC, ACTA: The Anti-Counterfeiting Trade Agreement, http://ec.europa.eu/trade/creating-opportunities/trade-topics/intellectual-property/anti-counterfeiting/

84. EESC, “OPINION of the European Economic and Social Committee on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Single Market for Intellectual Property Rights – Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe, COM(2011) 287 final”, Brussels, 1/18/2012, pp. 8, 3.1.3., and p. 10, 4.5.5. http://www.eesc.europa.eu/?i=portal.en.int-opinions.19154

85. http://www.mofa.go.jp/policy/economy/i_property/acta1201.html

86. http://thomas.loc.gov/cgi-bin/bdquery/z?d112:h.r.3261: for a list of those concerned about the legislation: https://www.cdt.org/report/list-organizations-and-individuals-opposing-sopa

87. http://keepthewebopen.com ; and http://keepthewebopen.com/assets/pdfs/faqs.pdf

88. http://keepthewebopen.com/assets/pdfs/faqs.pdf

89. Many companies struggle to ensure free expression while not jeopardizing political stability. Google removed the anti-Islam video that set off riots in Egypt, Libya and other countries, during the week of September 11, 2012. However, Google did not block the film everywhere. Google was also asked by the US Government to take down the video. Brian Womack, “Google’s YouTube Expands Anti-Islam Film Restriction in Asia,” Bloomberg News, 9/14/2012, http://www.bloomberg.com/news/2012-09-14/google-expands-anti-islam-video-restriction-to-india-indonesia.html

90. http://www.google.com/transparencyreport/removals/government/countries/ ; David Kravets, “Google Says It Removes 1 Million Infringing Links Monthly,” Wired, 5/24/2012, http://www.wired.com/threatlevel/2012/05/google-infringing-link-removal/?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=MoreRecently

91. NA, “US, Colombia Discuss Implementation Of IP Provisions Due Next Year,” Inside US Trade, 6/08/12.

92. Charlotte Waelde and Lilian Edwards, “Online Intermediaries and Copyright Liability,” WIPO Workshop Keynote Paper, Geneva, April 2005, pp. 35, 51-52. http://ssrn.com/abstract=1159640

93. “Colombian Senators File Lawsuits Against Copyright Bill Passed to Comply with Trade Agreement” 6/8/2011, http://infojustice.org/archives/26337

94. Jesse Brown, “Pirate Politics aren’t just for Hackers,” McLeans, 9/21/2011, http://www2.macleans.ca/2011/09/21/pirate-politics-arent-just-for-hackers/

95. http://www.pp-international.net/about; pirate codex http://www.pirates-without-borders.org/pirates-codex/; and Josh Kron, “Open Source Politics: The Radical Promise of Germany’s Pirate Party,” The Atlantic.com 9/21/2012, http://www.theatlantic.com/international/archive/2012/09/open-source-politics-the-radical-promise-of-germanys-pirate-party/262646/?single_page=true

96. http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=noticeandaction

97. EC, “A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries,” http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-Internet_en.htm

98. NA, “UK continues to oppose new single EU data protection law regime,” Out-law.com, 11/13/2012, http://www.out-law.com/en/articles/2012/november/uk-continues-to-oppose-new-single-eu-data-protection-law-regime/

99. EU, “Strategy for the Enforcement of Intellectual Property Rights in Third Countries,” 2005/C 129/03, p. 14, at http://trade.ec.europa.eu/doclib/docs/2010/december/tradoc_147070.pdf

100. EU-Korea is at http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2011:127:SOM:EN:HTML; The EU /Asean negotiations are being paused due to rampant piracy and other factors. NA, “EU gives ASEAN 4.5 million euros for intellectual property,” Deutsche Presse Agentur, 10/21/2009, http://www.bilaterals.org/spip.php?article16126

101. Jason J. Lee, “Enactment of Korea-EU Free Trade Agreement triggers amendments to IP laws,”, 1/12/2012, http://www.bilaterals.org/spip.php?article20890

102. After a February draft of the EU/Canada FTA was leaked an EU spokesman said that it would not require Internet service providers to post names online of individuals alleged to have breached copyright (as in ACTA). However, in late September, EU member states supposedly received an email that informed EU officials that the trade agreement had criminal sanctions for online copyright infringement similar to those in ACTA. https://twitter.com/EUJohnClancy/statuses/222999382851723264; and David Meyer, “Canada trade deal no longer borrows from ACTA: EU,” ZDNet, 7/11/2012, http://www.zdnet.com/canada-trade-deal-no-longer-borrows-from-acta-eu-7000000700/

103. For information on the digital economy in Canada, see http://www.digitaleconomy.gc.ca/eic/site/028.nsf/eng/home

104. Paul Chwelos, “Internet Service Providers Report, Executive Summary”, 2009, http://www.ic.gc.ca/eic/site/ippd-dppi.nsf/eng/ip01431.html

105. NA, "Letting the baby dance," Economist, 9/1/2012, http://www.economist.com/node/21561885

106. Web site Law Professor Michael Geist, Canada Research Chair in Internet and E-commerce Law, University of Toronto, http://www.michaelgeist.ca/content/view/6588/125/; and Nancy Situ, "Considering Canada's Supreme Court Decisions In This Week's WIPO Proceedings," http://www.ip-watch.org/2012/07/18/considering-canadas-supreme-court-decisions-in-this-weeks-wipo-proceedings/

107. Canada/Colombia, "E-commerce chapters", http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/colombia-colombie/chapter15-chapitre15.aspx?view=d

108. American Assembly, " Copyright Infringement and Enforcement in the US, A Research Note, 11/2011," p. 9, http://piracy.americanassembly.org/wp-content/uploads/2011/11/AA-Research-Note-Infringement-and-Enforcement-November-2011.pdf.

109. Issos polled 7,087 adults and 1,787 teenagers from Australia, Brazil, China, France, India, Indonesia, Japan and the United States. Patricia Reaney, "Online Sharing, Information Overload is Worldwide Problem: poll," Reuters, 9/5/2012, http://www.reuters.com/article/2012/09/05/net-us-technology-mobile-poll-idUSBRE8840NF20120905

110. Waelde and Edwards found ISPs are too receptive to takedown. They also need to maintain extensive staff to ensure they are not breaching privacy or copyright. Charlotte Waelde and Lilian Edwards, "Online Intermediaries and Copyright Liability," WIPO Workshop Keynote Paper, Geneva, April 2005, pp. 30-31. http://ssrn.com/abstract=1159640

111. NA, "Letting the baby dance," Economist, 9/1/2012, http://www.economist.com/node/21561885

112. Emma Barnett, "Facebook's Mark Zuckerberg says privacy is no longer a 'social norm'," The Telegraph, 1/11/2010, http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html

113. For an interesting analysis of this issue, see Michael Geist and Milana Homsi,"Outsourcing Our Privacy?: Privacy and Security in a Borderless Commercial World," University of New Brunswick Law Journal Vol. 54, 2005.

114. Privacy Canada, "Privacy for Everyone, Annual Report to the Parliament,2011, Report on the *Personal Information Protection and Electronic Documents Act*, http://www.priv.gc.ca/information/ar/201112/2011_pipeda_e.asp#toc3.5

115. Soumitra Dutta, William H. Dutton, and Ginette Law, "The New Internet World: A global Perspective on Freedom of Expression, Privacy, Trust and Security Online," 4/2011, 9-11. The researchers analyzed public opinion on privacy in Australia/New Zealand, Brazil, Canada, China, France, Germany, Italy, India, Mexico, South Africa, Spain, the US and the U.K.

116. Ian Brown, "Privacy Attitudes, Incentives and Behaviors," 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1866299&

117. Sweden was the first government to establish privacy legislation and today there are some 80 countries/entities with such laws. Steven Bellman et al, "International Differences in Information Privacy Concerns: A Global Survey of Consumers," Information Society, 20, (2004): 313-324, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1324721&

118. On US court cases see, Martin Samsun, Internet Library of Law and Court Decisions, http://www.Internetlibrary.com/topics/right_privacy.cfm; on Sarbanes-Oxley, see Public Law 107 - 204 - Sarbanes-Oxley Act of 2002, at http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html

119. The Department of Commerce Internet Policy Task force, "Commercial Data Privacy and Innovation in the Internet Economy," p. 44, p. 54. http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf

120. "Conference on Current Developments in Privacy Frameworks: Towards Global Interoperability," hosted by Ministry of Economy of Mexico, 11/1/2011, http://www.oecd.org/document/23/0,3746,en_2649_34223_48443927_1_1_1_1,00.html#Agenda

121. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

122. The Council of Europe promotes common and democratic principles based on the European Convention on Human Rights and other reference texts on the protection of individuals. It is also home to the European Court of Human Rights, which clarifies European law related to human rights. Doc. 12695, 29 July 2011, "The protection of privacy and personal data on the Internet and online media," Report, Committee on Culture, Science and Education Rapporteur: Ms Andreja Rihter, Slovenia, Socialist Group, http://www.assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=13151&Language=EN

123. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention No. 108") requires that personal data be processed fairly and securely for specified purposes on a legitimate basis only, and establishes that everyone has the right to know, access and rectify their personal data processed by third parties or to erase personal data which have been processed without authorisation. The EU has not however devised an action plan for implementing Convention 108.

124. www.futureofprivacy.org/global; and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

125. US Department of Commerce, "Safe Harbor," http://export.gov/safeharbor/eu/eg_main_018476.asp

126. Interview with Rosa Barcelo, Privacy Coordinator, Policy Coordinator , European Commission, DG CONNECT, 7/24/2012. Also see Gregory Shaffer, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Data Privacy Standards," Yale Journal of International Law 25, Winter 2000, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=531682.

127. Regarding Philippine adoption of legislation, based on the EU Data Protection Directive 95/46/EC and accords with APEC policies, NA, "Senate Ratifies Bicam Report on Data Privacy Act," Zambo Times, 6/6/2012, http://www.zambotimes.com/archives/48155-Senate-ratifies-bicam-report-on-Data-Privacy-Act.html

128. Neil Robinson et al, for Rand Europe, "Review of the European Data Protection Directive 39," 2009,

129. European principles and guidelines for Internet resilience and stability, March 2011, http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_Internet_fin.pdf

130. European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 1/12/2012, COM(2012) 11 final http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

131. Press Release, "Data Protection Reform: Frequently Asked Questions," Memo/12/41/ Brussels, 25 January 2012, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/41&format=HTML&aged=0&language=EN&guiLanguage=fr; EC, "Why do we need an EU Data Protection Reform," http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf; and EC, "How will the EU's data protection reform make international cooperation easier?" http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_en.pdf

132. http://trade.ec.europa.eu/doclib/docs/2008/february/tradoc_137971.pdf. Canada has similar provisions.

133. Chapter 6 of its model free Trade Agreements refer to trade in data. http://trade.ec.europa.eu/doclib/docs/2008/february/tradoc_137971.pdf.Article 7.43 http://trade.ec.europa.eu/doclib/docs/2009/october/tradoc_145166.pdf

134. http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights . The bill of rights includes a right to transparency: Consumers have a right to easily understandable information about privacy and security practices; **Respect for Context:** Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data; **Security:** Consumers have a right to secure and responsible handling of personal data; **Access and Accuracy:** Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate; **Focused Collection:** Consumers have a right to reasonable limits on the personal data that companies collect and retain; and **accountability:** Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

135. Cameron S. Kerry "Second Annual European Data Protection and Privacy Conference, CFK Keynote Address, Transatlantic Solutions for Data Privacy," 12/6/2011, . http://www.ntia.doc.gov/speechtestimony/2011/cameron-f-kerry-keynote-address-european-data-protection-and-privacy-conference. Kerry, the Commerce Department's General Counsel, noted some 3000 companies participate in Safe Harbor with the EU; he also stressed theat the US adopted the Asia Pacific Economic Cooperation's Cross Border Privacy Rules.

136. The Department of Commerce Internet Policy Task force, "Commercial Data Privacy and Innovation in the Internet Economy P. 44, p. 54. http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf and Department of Commerce, export.gov, Introduction to the US-Eu and US Swiss Safe Harbor Frameworks, www.export.gov/safeharbour.

137. U.S Department of Commerce, "2009 Electronic Commerce Industry Assessment," http://web.ita.doc.gov/ITI/itiHome.nsf/0657865ce57c168185256cdb007a1f3a/3771d41ba49c5cba852577440056dcd4/$FILE/Electronic Commerce Industry Assessment Public June 16.pdf

138. Article 15.5 of US/Panama FTA, http://www.ustr.gov/sites/default/files/uploads/agreements/fta/peru/asset_upload_file876_9540.pdf

139. US Department of Commerce, "US-EU Joint Statement on Privacy from EU Commission Vice President Viviane Redding and US Commerce Secretary John Bryson," 3/19/2012.

140. Message from the Privacy Commissioner of Canada, http://www.priv.gc.ca/aboutUs/message_e.cfm#contenttop

141. Office of the Information and Privacy Commissioner for British Columbia, 2011-12 Annual Report, 6-7.

142. Office of the Privacy Commissioner of Canada, Guidelines for Processing Personal Data Across Borders, January 2009, http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp

143. Privacy Commissioner of Canada, "Privacy for all," http://www.priv.gc.ca/information/ar/201112/2011_pipeda_e.asp#toc1

144. Canada-Colombia Free Trade Agreement, Chapter Fifteen, Electronic Commerce, http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/colombia-colombie/chapter15-chapitre15.aspx?view=d

145. Information Technology Association of Canada, "Shared Services Canada takes National Security Exception," http://itac.ca/news/shared_services_canada_takes_national_security_exception

146. Jason Young, "BC Attempts to Regulate outsourcing of Personal Information," 11/4/2004, http://www.dww.com/?page_id=1052; and Fred H. Cate, "Provincial Canadian Geographic Restrictions on Personal Data in the Public Sector," Centre for Information Policy Leadership, Submitted to the Trilateral Committee on Transborder Data Flows, 2008, pp. 1-2.

147. Fred H. Cate, "Provincial Canadian Geograhpical Restricttions on Personal Data in the Public Sector, Center for Information Leadership, Hunton and Williams, http://www.hunton.com/files/Publication/2a6f5831-07b6-4300-af8d-ae30386993c1/Presentation/PublicationAttachment/0480e5b9-9309-4049-9f25-4742cc9f6dce/cate_patriotact_white_paper.pdf

148. Office of the Information and Privacy Commissioner for British Columbia, 2011-12 Annual Report, 6-7.

149. Privacy Commissioner of Canada, "Privacy for all," http://www.priv.gc.ca/information/ar/201112/2011_pipeda_e.asp#toc1

150. FAC, "Obama Acts on FAC petition against China's "Great Firewall" 10/19/2011, http://www.firstamendmentcoalition.org/2011/10/obama-acts-on-fac-petition-against-chinas-Internet-censors/.

151. Brendan Greeley and Mark Drajem, "China's Facebook Copycats Focus US on Trade as Well as Rights," Bloomberg/Business Week, 3/10/2011 and Letter from Ambassador Michael Puncke, US Ambassador to the WTO to Ambassador Yi Xiaozhun, China's Ambassador to the WTO, and Attachment, 10/17/2011, at http://insidetrade.com/iwpfile.html?file=oct2011%2Fwto2011_2996a.pdf .

152. NA, "USTR Flags Procurement, Data Flow Issues as New Barriers in Canada," Inside US Trade,4/27/2012

153. USTR, National Trade Estimate Report, 2012 http://www.ustr.gov/sites/default/files/NTE Final Printed_0.pdf. "A number of US companies have voiced concerns that various Australian government departments, such as the Department of Defense, the National Archives of Australia, the Department of Finance and Deregulation Australian Government Information Management Office, and the State of Victoria Privacy Commissioner, are sending negative messages about cloud computing services to potential Australian customers in both the public and private sectors, implying that hosting data overseas, including in the United States, by definition entails greater risk and unduly exposes consumers to their data being scrutinized by foreign governments. In the case of the United States, many such concerns appear based on misinterpretation of applicable US law, including the US Patriot Act and regulatory requirements. In November 2011, new draft legislation was introduced into Parliament that would prohibit the overseas storage of any Australian electronic health records. This would pose a significant trade barrier for US information technology companies with data centers located in the United States or anywhere else outside of Australia. The bill has been referred to a Senate committee for inquiry."

154. USTR, National Trade Estimate Report, 2012 p. 216, http://www.ustr.gov/sites/default/files/NTE Final Printed_0.pdf

155. USTR, National Trade Estimate Report, 2012 p. 96, http://www.ustr.gov/sites/default/files/NTE Final Printed_0.pdf

156. Edward J. Black, President, Computer and Communications Industry Association, to House Ways and Means Committee, 6/19/2012 re. Internet Freedom and Granting Russia Permanent Normal Trade Relations

157. NA, "Finance Russia MFN Bill Expands Special 301 Report To Digital Freedom,"Inside US Trade, 7/19/2012, According to Inside US Trade, "The new requirement for future versions of the report, championed by Sen. Ron Wyden (D-OR), comes after the Russian Duma voted to establish a blacklist of websites that its government could shut down. US technology companies represented by the Computer & Communications Industry Association and others are opposing these Russian measures. The new requirement on digital trade, could be used to trigger a challenge in the World Trade Organization if USTR were to designate a foreign trading partner as a "priority foreign country" due to gross IPR violations. USTR has largely refrained from doing so in the past under both Democratic and Republican administrations." For the House bill, see http://insidetrade.com/iwpfile.html?file=nov2012%2Fwto2012_2422b.pdf

158. USTR, National Trade Estimate Report, 2012, 166, http://www.ustr.gov/sites/default/files/NTE Final Printed_0.pdf

159. Although the US argued it had to discriminate between domestic and foreign gambling web sites to avoid fraud, money laundering, and organized crime, the US lost a trade dispute on this issue at the WTO.United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services, http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm; and Albena P. Petrova, "The WTO Internet Gambling Dispute as a case of First Impression: How to Interpret Exceptions Under GATS Article XIV (a)…" Richmond Journal of Global Law and Business, 6:1, pp. 45-76, http://rjglb.richmond.edu/archives/6.1/art2.pdf

160. Jian Junbo, "Internet Claims too Testy for China," Asia Times, 5/27/2010, http://www.atimes.com/atimes/China/LE27Ad01.html

161. Commission Staff Paper Accompanying the Trade and Investment Report, http://trade.ec.europa.eu/doclib/docs/2012/february/tradoc_149144.pdf; and REPORT FROM THE COMMISSION TO THE EUROPEAN COUNCIL "Trade and Investment Barriers Report 2012" {SWD(2012) final} 19, http://trade.ec.europa.eu/doclib/docs/2012/february/tradoc_149143.pdf, pp. 9, 15-16

162. NA, "Iran's Twitter Revolution," Washington Times 06/16/2009, http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/; and Zoe Fox, "How the Arab World Uses Facebook and Twitter," Mashable 6/8/2012, http://mashable.com/2012/06/08/arab-world-facebook-twitter/

163. For the example of riots in the UK, see http://www.reuters.com/article/2011/08/09/us-britain-riots-blackberry-i https://www.nytimes.com/2011/08/12/world/europe/12iht-social12.html?_r=1 dUSTRE7784EE20110809; http://www.aljazeera.com/indepth/opinion/2012/04/201241373429356249.html; Anthony Faiola, "London Riots: Britain Weighs Personal Freedoms against Need to Keep order," 8/11/2011, http://www.washingtonpost.com/world/europe/britain-weighs-personal-freedoms-against-need-to-keep-order/2011/08/11/gIQAMTOS8I_print.html. For the example of India, see Gardiner Harris and Malavika Vyawahare, "Indian Government Defends Social Media Crackdown," http://india.blogs.nytimes.com/2012/08/24/indian-government-defends-social-media-crackdown/

164. https://twitter.com/JeanBirnbaum/status/226348204160065537

165. NA, "BIS Offers Enhanced Enforcement Plan For Items Subject To Reform Effort", Inside US Trade, 7/19/2012

166. James Ball, "Sanctions aimed at Syria and Iran are hindering opposition, activists say," Washington Post, 8/14/2012, http://www.washingtonpost.com/world/national-security/sanctions-aimed-at-syria-and-iran-are-hindering-opposition-activists-say/2012/08/14/c4c88998-e569-11e1-936a-b801f1abab19_story.html

167. VOA, "The US Boosts Exports of Internet Services to Closed Societies," 3/10/2010, https://www.youtube.com/watch?v=qLDIQzpd5kcpress06252010.htm

168. "BIS Updates Encryption Export Rule; Revised Rule Streamlines Review Process, Enhances National Security," Department of Commerce Bureau of Industry and Security (25 June 2010), http://www.bis.doc.gov/news/2010/bis_press06252010.htm

169. Amy Chozick, "Offical Syrian Web Sites Hosted in the United States," NY Times 11/30/2012, http://www.nytimes.com/2012/11/30/world/middleeast/official-syrian-web-sites-hosted-in-us.html; and Ron Deibert et al., "the Canadian Connection: One Year Later," https://citizenlab.org/2012/11/the-canadian-connection-one-year-later/444

170. http://www.state.gov/secretary/rm/2011/12/178511.htm; http://www.state.gov/j/drl/rls/rm/2012/180958.htm

171. http://geneva.usmission.gov/us-hrc/Internet-freedom-fellows-2012/

172. http://globalnetworkinitiative.org/

173. http://Internetfreedomfund.tumblr.com/

174. http://cordis.europa.eu/fp7/ict/fire/events/20120507-fire-nds-ws/ppts/01-no-disconnect-strategy-20120507-ag1.pdf

175. Ryan Gallagher, "EU Plans Groundbreaking Project To Monitor Internet Censorship Around the World," Slate, 11/6/2012, http://www.slate.com/blogs/future_tense/2012/11/06/european_capability_for_situation_awareness_program_to_monitor_internet.html

176. Deputy Assistant Secretary Dan Baer, "Live at State: Internet Freedom and US Foreign Policy," http://www.state.gov/r/pa/ime/178707.htm; and as example of technology project the USG funds, see For example, the US funds the TOR project, designed to help individuals use the Internet anonymously. http://en.wikipedia.org/wiki/The_Tor_Project. Also see Jay Newton-Small, "Hillary's Little Startup: how the US Is Using Technology to Aid Syria's Rebels," Time World, 6/13/2012, http://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/

177. See https://crypto.cat/; and debate at http://www.wired.com/threatlevel/2012/07/crypto-cat-encryption-for-all/all; and http://www.wired.com/threatlevel/2012/08/wired_opinion_patrick_ball/all//

178. Richard Fontaine and Will Rogers, "Internet Freedom: A Foreign Policy Imperative in the Digital Age," Center for a New American Security, 6/2011, 12, 13.

Photo and graphics credits:

p.3 ("Viva") by Flickr user Brunocandelas us under CC license; https://secure.flickr.com/photos/brunocandelas/6405380947/sizes/m/in/photostream/

p. 10 ("Do not want") by Flickr user RIUM+ used undder CC license: https://secure.flickr.com/photos/riumplus/3119688659/sizes/m/in/photostream/

p. 11 ("Piratpartiet") by Flickr user Anne Kekki, used under CC license; https://secure.flickr.com/photos/45937564@N02/4255043252/sizes/l/in/photostream/

p. 17 ("Dove") by Flickr user verbeeldingskr, used under CC license; https://secure.flickr.com/photos/verbeeldingskr8/4274218384/sizes/o/in/photostream/

p. 18 ("Threats") by Mozilla; used by permission.

p. 19 ("Switch") by Flickr user Mike Licht, NotionsCapital.com, used under CC license; https://secure.flickr.com/photos/notionscapital/5399168298/sizes/o/in/photostream/

p. 21 ("Sanal") by Flickr user Kevglobal, used under CC license; http://www.flickr.com/photos/kevglobal/5742334920/