

CICERO FOUNDATION GREAT DEBATE PAPER

No. 13/01

February 2013

**INTERNET GOVERNANCE
OR INTERNET CONTROL?**

HOW TO SAFEGUARD INTERNET FREEDOM

SUSAN ARIEL AARONSON

Associate Research Professor

Institute of International Economic Policy (IIEP)

Elliott School of International Affairs

George Washington University

Minerva Chair, National War College

Cicero Foundation Great Debate Paper No. 13/01

© Susan Ariel Aaronson, 2013

All rights reserved

The Cicero Foundation is an independent pro-Atlantic and pro-EU think tank.

www.cicerofoundation.org

The views expressed in Cicero Foundation Great Debate Papers do not necessarily express the opinion of the Cicero Foundation, but they are considered interesting and thought-provoking enough to be published. Permission to make digital or hard copies of any information contained in these web publications is granted for personal use, without fee and without formal request. Full citation and copyright notice must appear on the first page. Copies may not be made or distributed for profit or commercial advantage.

The Cicero Foundation

FRANCE

13, rue Washington

75008 PARIS

Tel. +33 1 45 62 05 90

Fax +33 1 45 62 05 30

Email info@cicerofoundation.org

THE NETHERLANDS

Hondertmarck D 45

6211 MB MAASTRICHT

Tel. +31 43 32 60 602

Fax +31 43 32 60 828

cicerofoundation@gmail.com

CONTENTS

Introduction 4

Location 9

Intellectual Property Rights (IPR) Enforcement 12

Intellectual Property Rights Provisions in the EU 17

The Future Direction of Strategies to Enforce Online IPR 19

Data Protection, Laws, Privacy, and Trade 20

Privacy Regulations in the EU 21

Privacy Regulations in the US 23

Challenging Internet Regulation a Barrier to Trade 24

The Position of the US 24

The Position of the EU 26

Promoting Internet Freedom Abroad 26

Export Bans: US and EU 26

Promoting Internet Freedom: US and EU 28

Promoting Internet Freedom: Conclusions 30

Notes 31

Internet Governance or Internet Control? How to Safeguard Internet Freedom

Susan Ariel Aaronson

Introduction

The Internet is simultaneously enhancing and restricting human welfare. On one hand, the Internet is creating a virtuous circle of expanding growth, opportunity, and information flows.¹ At the same time, policymakers and market actors are taking steps that undermine access to information, reduce freedom of expression and splinter the Internet.² 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.³ 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 the open Internet.

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.

Yet policymakers and netizens alike have not devised effective policies to ensure that the Internet has mainly positive benefits. 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 or spam etc...

Herein I examine how the US and the EU **use trade policies to govern the Internet at home and across borders**. The 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.

Attitudes towards Internet governance -- how has trade policy become a tool to regulate the Internet?

The US and the EU 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 and the EU

have fundamentally different approaches to Internet governance at the national level and in trade agreements.⁴

Moreover, the 2 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,⁵ 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 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 Chinese⁶ and Russian governments⁷ 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.⁸ The Chinese and Russian governments have become increasingly vocal about rethinking Internet governance and have proposed greater international control over the Internet.⁹ At the same time, many developing countries are just beginning to set the ground rules for the Internet in their countries.¹⁰ 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.¹¹ Officials in these countries make the case that greater governmental control will help them provide public goods

online such as education and healthcare, and to foster innovation and economic growth throughout their country.¹²

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.¹³ The US and the EU 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.¹⁴ However, these principles are neither universal nor binding. Hence, government officials have sought other venues to address cross-border Internet issues.

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.¹⁵ 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 and European business. Moreover, 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.¹⁶ US and European 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.¹⁷ They can achieve these internationally accepted rules within bilateral, regional, or broader multilateral trade agreements.¹⁸

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 the rule of law on international trade.

The WTO is a set of rules delineating 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 telecommunication networks, and to harmonize telecommunications policies that can affect international trade.¹⁹ Although the WTO does not explicitly regulate Internet services per se, it regulates trade in the goods and services that comprise e-commerce.²⁰ Some 74 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.²¹ 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).²² Alas, the member states have not found common ground on how to reduce new trade barriers to information flows.²³ In 2011, several nations nixed a US and the EU proposal that members agree not to block Internet service providers or impede the free flow of information online.²⁴ 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.²⁵

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.²⁶ As a result, individuals and firms involved in online transactions have no way to directly represent their interests at the WTO. Secondly, information is a global public good; access to information is a basic human right under international human rights law, and hence governments have a responsibility to ensure that their citizens have access to information through transparency mechanisms.²⁷ The WTO does have clear rules on transparency, due process, and political participation related to trade rulemaking.²⁸ But the WTO does not address human rights and it 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 privacy²⁹ or the right to free expression.³⁰ Thirdly, 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 but more about achieving interoperability among different governance approaches.³¹

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 and the EU 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.³²

Location

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.³³ 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.³⁴ 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 U.S. 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.³⁵ 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,³⁶ the US and 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.³⁷ The language in this FTA was extensive. First, the two nations agreed to accept electronic signatures and included provisions designed to protect consumers online.³⁸ Secondly, the two nations agreed to

encourage free flow. 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*”³⁹ 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.⁴⁰ 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.⁴¹

Officials from some of the TPP parties have not responded enthusiastically to these provisions. Some of the countries in the negotiation, such as Vietnam, have extensive restrictions on the Internet. Moreover, some TPP countries and individuals have expressed fears that this requirement that e-commerce platforms not be located at home is a national security or protectionist issue.⁴²

The US may be encountering significant opposition to these 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 that data can flow freely across borders with some narrowly tailored 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.⁴³ However, these countries have not yet had a domestic debate about how to balance these policy goals and may not be ready to discuss these issues internationally.

Meanwhile, the US and the EU 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.⁴⁴ 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 Trade Representative (USTR) and the EU 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.⁴⁵

Intellectual Property Rights Enforcement

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 have created a wide range of communities to share information online. However, sometimes netizens share copyrighted information online without respecting the intellectual property rights of content creators.⁴⁶

Under US and EU 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.⁴⁷ This

agreement helped reduce non-tariff trade barriers stemming from different IPR regimes and 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 understanding of how people would share information online.⁴⁸ 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).

Policymakers designed US copyright laws to protect rights holders, to encourage the creation of new knowledge, and to protect intermediaries. 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 1976.⁴⁹ Software developers, educational institutions, Internet search portals and others depend on 'fair use' to provide or adapt information for consumers, students, and users.⁵⁰ Several analysts have shown that these 'fair use' provisions contribute to economic growth because individuals and firms learn from and built on the work of others.⁵¹ (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'.⁵²) 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.⁵³

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.⁵⁴ However, the IPR chapters do not always include all of the attributes of US copyright laws. Moreover, other countries have different approaches to protecting IPR and to judging infringement.

The US Trade Representative has developed increasingly stringent enforcement language in its trade agreements. For example, in the 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.⁵⁵ 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.⁵⁶ 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.⁵⁷

U.S. policymakers recognize that language protecting online copyright in FTAs will not be sufficient to prevent online privacy. The U.S. 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 other enforcement strategies.⁵⁸ First, a senior US official now serves as the Intellectual Property Enforcement Coordinator in the White House.⁵⁹ Her office reports on threats to United States intellectual property from criminal violation.⁶⁰ 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.⁶¹ Thirdly, the US also lists countries and web sites as "notorious markets" markets in which pirated or counterfeit goods are reportedly available.⁶² However, the Congressional Research Service reports this approach is not deterring online piracy.⁶³ The US government and US firms have increasingly sued users and file sharing sites.⁶⁴ The US has also taken steps to move the reach of US law beyond US borders. It has targeted middlemen who set up web sites that share links to free access to copyright material across borders, such as Mega-upload, and charged these individuals or companies with violating the Digital Millennium Copyright Act.⁶⁵ However, legal scholars and the courts are debating if the law has extraterritorial application.⁶⁶

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.⁶⁷

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 net-based protests, several EU governments announced that they no longer support ACTA.⁶⁸ In late February, 2012 the European Commission announced that it was suspending consideration of the agreement and referred it to the European Court of Justice.⁶⁹ 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."⁷⁰ Meanwhile, although the US Trade Representative insists the Congress does not have to approve ACTA, some members of Congress disagree.⁷¹

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.⁷² 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. 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.⁷³ 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."⁷⁴ 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 focuses and 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 90percent of requests.⁷⁵ In May, 2012, Google said it had received 1.24 million requests from 1,296 copyright owners for removal, targeting 24,129 domains.⁷⁶ 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 a clear due process procedure 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 these issues. 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."⁷⁷

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.⁷⁸

Intellectual Property Rights Provisions in the 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 its own decisions about when to remove content for violations of IPR.

Citizens in the many European countries have become increasingly concerned about the focus on enforcement of IPR rights 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.⁷⁹ Pirate Party members hold two seats in the European Parliament and several seats in state Parliaments in Germany.⁸⁰

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.⁸¹ EC 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.⁸² However, the UK, Denmark, Slovenia, Belgium, Hungary and Sweden are opposed to an EU- wide regulation and prefer to have a directive, which would allow common rules and maintain individual state flexibility in administrating online IPR, as before.⁸³

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 copyright 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.”⁸⁴ 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.⁸⁵ 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.⁸⁶

As noted above, the EU and Canada are also negotiating an FTA. Because the FTA's provisions have not been made public or have not been leaked, we don't know if the agreement will include strong enforcement language such as that in ATCA.⁸⁷

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.⁸⁸ At the same time, a 2012 poll commissioned by Intel of web users in 8 countries found that 60 percent of those surveyed admitted that they "over share" online.⁸⁹

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.⁹⁰

Policymakers are increasingly responsive to these concerns. For example, the UK and New Zealand are rethinking their approach to copyright on and offline.⁹¹

Data Protection, Laws, Privacy, and Trade

In 2010, Facebook CEO Mark Zuckerberg said that “privacy is dead” because of the Internet.⁹² Zuckerberg may be wrong; netizens are increasingly demanding that government protect their data online. As consumers and citizens, they are both winners and losers in the flow of information that is collected, processed, and analyzed across borders.⁹³ They benefit from cheaper and greater access to information; but their information may not be secure. However, many netizens rely on the same few platforms. When such a platform has a privacy brief, it can affect millions of people around the world.⁹⁴

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.⁹⁵ 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.⁹⁶ However, barriers to trust are also barriers to access. As privacy is an issue of trust among online market actors, EU and US policymakers must balance protecting privacy with rules governing cross-border data flows.

The US and the EU have different definitions of privacy and distinct strategies to protect it. The US sees privacy as a consumer right. Europeans see privacy as both a human and consumer right.⁹⁷ 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.⁹⁸

Nonetheless, American and European 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 its 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.⁹⁹ 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.¹⁰⁰ 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.¹⁰¹ 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 Regulations in the 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.¹⁰² Every EU citizen has the right to personal data protection and firms can only collect that

data under specific conditions.¹⁰³ The EU also requires member states to investigate privacy violations.¹⁰⁴

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.¹⁰⁵

The EU Directive has had an effect on trade. Because of the importance of cross-border data flows to/from the 27 countries of the EU, some nations such as India and China are weighing how to make their laws interoperable with EU privacy provisions.¹⁰⁶ Meanwhile, other countries such as the Philippines have adopted EU data protection policies.¹⁰⁷

Some observers of the EU approach assert that the EU focuses on process rather than outcomes or on promoting "effective good data protection practices."¹⁰⁸ The EC has decided to update its data protection rules to meet changes in technology and increased public concern about privacy.¹⁰⁹ After obtaining extensive public comment, the EU parliament is now considering a regulation developed by European Commission staff.¹¹⁰ 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.¹¹¹

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 says; 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."¹¹² 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.¹¹³

Privacy Regulations in the US

In contrast with the EU, 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 enforceable privacy policies based on this proposed bill of rights.¹¹⁴ The US plans to make its new approach to privacy interoperable with the privacy frameworks of its international partners.¹¹⁵

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) 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.¹¹⁶ 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.¹¹⁷

The US has included language related to consumer protection in its FTAs, but has not mentioned privacy as an objective or included specific privacy language. As an example, in the e-commerce chapters such as that for US/Panama, the agreement states that the parties recognize the importance of protecting consumers online and will cooperate on privacy.¹¹⁸ 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."¹¹⁹

Challenging Internet Regulations as Barriers to Trade

The Position of the 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 initiating 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.¹²⁰ 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.¹²¹

The US has also identified privacy rules as a barrier to the free flow of information in Canada and Australia.¹²² 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.¹²³ The US also complained about Japan's uneven approach to privacy and Vietnam's unclear approach.¹²⁴ Ironically, the US also argues that China's failure to enforce its privacy laws stifles e-commerce.¹²⁵

As of November 2012, Congress is considering legislation to apply normal trade relations to Russia and Moldova.¹²⁶ 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.¹²⁷

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.”¹²⁸

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 objective seems reasonable, the dispute settlement body found that the US was discriminating among foreign and domestic purveyors of internet gambling.¹²⁹

The Position of the EU

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.¹³⁰ The EU does not target other countries privacy policies as trade barriers, although it does view national security policies as potential barriers to trade. Hence the EU response to the Patriot Act described above, although the EU did not formally cite this legislation as a formal barrier in its official annual report. However, 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.¹³¹

Promoting Internet Freedom Abroad

Export Bans: US and EU

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.¹³² 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.¹³³

The two trade giants have considerable leverage. 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 and US 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.¹³⁴ US and EU officials have sanctioned bad actors and limited access to goods or services that government officials 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.¹³⁵

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.¹³⁶

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.¹³⁷ The US also eliminated export restrictions on "mass-market electronic products with encryption functions such as laptops and cell phones."¹³⁸

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. Yet, in so doing, the US is further restricting the Internet at home supposedly in the interest of punishing the Syrian government. The Department of State claimed this would promote the ability of Syrians to exercise their freedom of expression, although it is unclear how.¹³⁹ European countries also hosted some of these sites.

None of the countries have developed clear guidance to their firms as to when they can sell general-use technologies or host sites for 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).

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 interests, 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.¹⁴⁰ 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.¹⁴¹ 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.¹⁴²

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.¹⁴³ 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."¹⁴⁴ With EU funding, EC officials are a "European Capability for Situational Awareness," to aggregate and visualize up-to-date intelligence about the state of the Internet across the world.¹⁴⁵ 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.¹⁴⁶ 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.¹⁴⁷

Promoting Internet Freedom: Conclusions

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 nor developed a clear and consistent argument as to why Internet freedom and openness are important to both economic growth and political stability.¹⁴⁸ 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.

NOTES

¹ 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

² 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.

³ <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>

⁴ The US approach to governance differs from that in the EU. 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. On Europe, Remarks of Marietje Schaake, 11/2/2012, at Congressional Internet Caucus Advisory Committee.

⁵ 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, <http://www.ecipe.org/publications/wcit/>, p. 3.

⁶ 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

⁷ 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. 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

⁸ 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/>

⁹ 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>

¹⁰ Scott J. Wallsten. "Regulation and Internet Use in Developing Countries" *Economic Development and Cultural Change* 53. #2 (2005): 501-523.

¹¹ 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?ito=feeds-newsxml%20%3Chttp://www.dailymail.co.uk/indiahome/indianews/article-2220692/How-India-helped-bunch-bureaucrats-custodians-Internet.html?ito=feeds-newsxml%3E](http://www.dailymail.co.uk/indiahome/indianews/article-2220692/How-India-helped-bunch-bureaucrats-custodians-Internet.html?ito=feeds-newsxml%3E);

¹² 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>

¹³ 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>

¹⁴ In June 2011, the thirty eight members of the OECD and Egypt agreed to the OECD Principles for Internet Policymaking. <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. See <http://www.government.nl/news/2011/12/14/coalition-of-countries-for-free-Internet.html>; and <http://www.freedomonlinekenya.org/home>

¹⁵ 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.

¹⁶ 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.

¹⁷ 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

¹⁸ 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%20pubs/Regional_Ecommerce.pdf

¹⁹ 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

²⁰ 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.

²¹ 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

²² 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

²³ 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

²⁴ 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.

²⁵ Data protection regulations are exempted from scrutiny under the GATS as long as these regulations are not a disguised restriction on trade.

²⁶ However, some of the WTO's disciplines directly affect commercial conduct, as example, delineating a telephone companies' obligation to treat customers in a non-discriminatory manner. I am grateful to USTR staff for that insight.

²⁷ 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>.

²⁸ 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.

²⁹ 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

³⁰ 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/castancentre/projects/wto/wto-lit-review-05.pdf>.

³¹ For an excellent overview, see Mira Burri and Thomas Cottier, editors, *Trade Governance in the Digital Age* (for the World Trade Forum) (New York, Cambridge U. Press), 2012.

³² 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.

³³ 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.

³⁴ NFTC, Promoting Cross-Border Data Flows: Priorities for the Business Community, 2011, <http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf>

³⁵ 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/speechtestimony/2011/remarks-us-chamber-commerce-global-flow-information-internet>

³⁶ Brian Bieron and Usman Ahmed, “Regulating E-commerce Through International Policy: Understanding the Trade law Issues of e-commerce,” *Journal of World Trade*, 46, no3 (2012):548-555.

³⁷ The agreement went into force in 2012.

³⁸ 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, p. 4-5 fn. 98, <http://www.usitc.gov/publications/pub3949.pdf>

³⁹ US/Korea FTA, Chapter 15, Article 15.8 Electronic Commerce, <http://www.ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text>

⁴⁰ Knowledge Ecology International to Senator Patrick Leahy, 1/26/2012, <http://keionline.org/node/1349>

⁴¹ NA, Inside US Trade, “TPP Countries to Discuss Australian Alternative to Data-Flow Proposal,” Inside US Trade, 7/5/2012, [Insidetrade.com/Inside-US-Trade/Inside-U.S.-Trade-07/06/2012/tpp-countries-to-discuss-australian-alternative-to-data-flow-proposal/menu-id-172.html](http://insidetrade.com/Inside-US-Trade/Inside-U.S.-Trade-07/06/2012/tpp-countries-to-discuss-australian-alternative-to-data-flow-proposal/menu-id-172.html)

⁴² http://www.brookings.edu/~media/events/2010/1/20%20cloud%20computing/20100120_cloud_computing, Remarks of Rob Atkinson. 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/

⁴³ NA, "USTR official: US Still Faces Big challenges on TPP Data Flow Proposal," *Inside US Trade*, 9/24/2012. <http://insidetrade.com/201209242411012/WTO-Daily-News/Daily-News/ustr-official-us-still-faces-big-challenges-on-tpp-data-flow-proposal/menu-id-948.html>

⁴⁴ NA, "Dreier Sees Less Enthusiasm In Congress For Outreach To EU Than TPP," *Inside US Trade*, 8/24/2012, <http://insidetrade.com/Inside-US-Trade/Inside-US-Trade-08/24/2012/dreier-sees-less-enthusiasm-in-congress-for-outreach-to-eu-than-tpp/menu-id-710.html>; and US, EU Seek To Tackle Trade Barriers In Advance Of HLWG Final Report, *Inside US Trade*, 10/19/2012, <http://insidetrade.com/Inside-US-Trade/Inside-US-Trade-10/19/2012/us-eu-seek-to-tackle-trade-barriers-in-advance-of-hlwg-final-report/menu-id-710.html>

⁴⁵ European Union-United States Trade Principles for Information and Communication Technology Service, 4/2012, http://www.ustr.gov/webfm_send/2780

⁴⁶ Executive Office of the President, 2011 U.S. Intellectual Property Enforcement Coordinator, "Annual Report on Intellectual Property Enforcement, 3/2012, 10-11.

⁴⁷ http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm,

⁴⁸ Google, (UK) "Submission to the Independent Review of Intellectual Property and Growth, 3/2011, p. 3, 3.5,

⁴⁹ The US Copyright Act is 17 USC. § 107. Much of the Internet industry grew under in the US under fair use.

⁵⁰ Thomas Rogers & Andrew Szamoszszegi, "Fair Use in the US Economy: Economic Contribution of Industries Relying on Fair Use," CClA, 2010), pp. 11-12, available online at [cclanet.org](http://www.cclanet.org/CCIA/files/cclibraryFiles/Filename/00000000354/fair-use-study-final.pdf). <http://www.cclanet.org/CCIA/files/cclibraryFiles/Filename/00000000354/fair-use-study-final.pdf>

⁵¹ Ibid, and CRS Report RL33631, *Copyright Licensing in Music Distribution, Reproduction, and Public Performance*, by Brian T. Yeh.

⁵² Bieron and Ahmed, "Regulating E-Commerce," 563.

⁵³ The Digital Millennium Copyright Act is P. L. 105-304.

⁵⁴ 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).

⁵⁵ 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

⁵⁶ 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

-
- ⁵⁷ Inside US Trade, "In Shadow Of ACTA, EU Drops Criminal IPR Provisions In CETA Talks," 11/2/2012, <http://insidetrade.com/Inside-US-Trade/Inside-U.S.-Trade-11/02/2012/in-shadow-of-acta-eu-drops-criminal-ipr-provisions-in-ceta-talks/menu-id-710.html>
- ⁵⁸ US industries such as software, music, films, and computer games rely on IPR protection. They lose billions of dollars in revenue from due to piracy and counterfeiting.
- ⁵⁹ The US also has a portal on its IPR policies and enforcement. www.iprcenter.gov
- ⁶⁰ 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%20Center%20Threat%20Report%20and%20Survey.pdf/view>
- ⁶¹ The Omnibus Trade and Competitiveness Act P. L. 100-418 included the Special 301 provisions.
- ⁶² USTR, "Out of Cycle Review of Notorious Markets," 2/28/2011, http://www.ustr.gov/webfm_send/2595
- ⁶³ 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.ieceusa.org/policy/eyeonwashington/2011/documents/iprtradeagreements.pdf>
- ⁶⁴ Torrent Freak, "first Software Maker Joins Bit-Torrent Lawsuit Bonanza," 11/16/2012, <http://torrentfreak.com/first-software-maker-joins-bittorrent-lawsuit-bonanza-121116/>
- ⁶⁵ 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](http://www.usdoj.gov) 1/19/2012. BBC News, "Megaupload extradition case delayed until March 2013," <http://www.bbc.co.uk/news/technology-18779866>
- ⁶⁶ 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), <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)
- ⁶⁷ 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>
- ⁶⁸ 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) 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>.
- ⁶⁹ 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/>
- ⁷⁰ 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, 1/18/2012, pp. 8, 3.1.3., and p. 10, 4.5.5.

⁷¹ http://www.mofa.go.jp/policy/economy/i_property/acta1201.html

⁷² <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>

⁷³ <http://keepthewebopen.com> ; and <http://keepthewebopen.com/assets/pdfs/faqs.pdf>

⁷⁴ <http://keepthewebopen.com/assets/pdfs/faqs.pdf>

⁷⁵ . 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-indonesia.html>

⁷⁶ 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

⁷⁷ NA, "US, Colombia Discuss Implementation Of IP Provisions Due Next Year," *Inside US Trade*, 6/08/12.

⁷⁸ Charlotte Waelde, Charlotte and Lilian Edwards, "Online Intermediaries and Copyright Liability," WIPO Workshop Keynote Paper, Geneva, April 2005, <http://ssrn.com/abstract=1159640> pp. 35, 51-52.

⁷⁹ 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/>

⁸⁰ <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. Qipte [/ 1-/

⁸¹ <http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=noticeandaction>

⁸² 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

⁸³ Outlaw.com, "UK continues to oppose new single EU data protection law regime," 11/13/2012, <http://www.out-law.com/en/articles/2012/november/uk-continues-to-oppose-new-single-eu-data-protection-law-regime/>

⁸⁴ 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

⁸⁵ 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. Deutsche Presse Agentur, "EU gives ASEAN 4.5 million

euros for intellectual property,” 10/21/2009, <http://www.bilaterals.org/spip.php?article16126>

⁸⁶ 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>

⁸⁷ <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-700000700/>

⁸⁸ 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>.

⁸⁹ 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>

⁹⁰ Edwards and Waelde found ISPs are too receptive to takedown. They also need to maintain extensive staff to ensure they are not breaching privacy or copyright. Edwards and Waelde, “Online Intermediaries and Liability for Copyright Infringement,” 30-31.

⁹¹ NA, “Letting the baby dance,” *Economist*.

⁹² 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>

⁹³ Michael Geist and Milana Homsy, “Outsourcing Our Privacy?: Privacy and Security in a Borderless Commercial World,” *University of New Brunswick Law Journal* Vol. 54, 2005.

⁹⁴ 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

⁹⁵ 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.

⁹⁶ Ian Brown, “Privacy Attitudes, Incentives and Behaviors,” 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1866299&

⁹⁷ 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&

⁹⁸ 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>

⁹⁹ 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>

¹⁰⁰ 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

¹⁰¹ The OECD Guidelines on the Protection of privacy and Transborder Flows of Personal Data, 1980.

¹⁰² 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>

¹⁰³ 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.

¹⁰⁴ 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>

¹⁰⁵ US Department of Commerce, "Safe Harbor," http://export.gov/safeharbor/eu/eg_main_018476.asp

¹⁰⁶ 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.

¹⁰⁷ Zambo Times, "Senate Ratifies Bicam Report on Data Privacy Act," <http://www.zambotimes.com/archives/48155-Senate-ratifies-bicam-report-on-Data-Privacy-Act.html>

¹⁰⁸ Neil Robinson et al, for Rand Europe, "Review of the European Data Protection Directive 39," 2009,

¹⁰⁹ 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

¹¹⁰ 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

¹¹¹ 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

¹¹² http://trade.ec.europa.eu/doclib/docs/2008/february/tradoc_137971.pdf.

-
- ¹¹³ 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
- ¹¹⁴ <http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights>
- ¹¹⁵ 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/spechtestimony/2011/cameron-f-kerry-keynote-address-european-data-protection-and-privacy-conference>.
- ¹¹⁶ 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.
- ¹¹⁷ U.S Department of Commerce, “2009 Electronic Commerce Industry Assessment,”
[http://web.ita.doc.gov/ITI/itiHome.nsf/0657865ce57c168185256cdb007a1f3a/3771d41ba49c5c8a852577440056dcd4/\\$FILE/Electronic%20Commerce%20Industry%20Assessment%20Public%20June%202016.pdf](http://web.ita.doc.gov/ITI/itiHome.nsf/0657865ce57c168185256cdb007a1f3a/3771d41ba49c5c8a852577440056dcd4/$FILE/Electronic%20Commerce%20Industry%20Assessment%20Public%20June%202016.pdf)
- ¹¹⁸ Article 15.5 of US/Panama FTA,
http://www.ustr.gov/sites/default/files/uploads/agreements/fta/peru/asset_upload_file876_9540.pdf
- ¹¹⁹ 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.
- ¹²⁰ 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/>. The US asked the Chinese questions related to who decides to filter the Internet and how are these decisions made?
- ¹²¹ 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/iwppfile.html?file=oct2011%2Fwto2011_2996a.pdf .
- ¹²² NA, USTR Flags Procurement, Data Flow Issues as New Barriers in Canada,” <http://insidetrade.com/Inside-US-Trade/Inside-US-Trade-04/27/2012/ustr-flags-procurement-data-flow-issues-as-new-barriers-in-canada/menu-id-710.html>
- ¹²³ USTR, National Trade Estimate Report, 2012
http://www.ustr.gov/sites/default/files/NTE%20Final%20Printed_0.pdf
- ¹²⁴ USTR, National Trade Estimate Report, 2012 p. 216
- ¹²⁵ USTR, National Trade Estimate Report, 2012 p. 96,
http://www.ustr.gov/sites/default/files/NTE%20Final%20Printed_0.pdf

-
- ¹²⁶ 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
- ¹²⁷ NA, "Finance Russia MFN Bill Expands Special 301 Report To Digital Freedom," Inside US Trade, 7/19/2012, and http://insidetrade.com/iwppfile.html?file=nov2012%2Fwto2012_2422b.pdf
- ¹²⁸ USTR, National Trade Estimate Report, 2012, 166, http://www.ustr.gov/sites/default/files/NTE%20Final%20Printed_0.pdf
- ¹²⁹ 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 Albenia 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>
- ¹³⁰ Jian Junbo, "Internet Claims too Testy for China," Asia Times, 5/27/2010, <http://www.atimes.com/atimes/China/LE27Ad01.html>
- ¹³¹ 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) 19 final} http://trade.ec.europa.eu/doclib/docs/2012/february/tradoc_149143.pdf, pp. 9, 15-16
- ¹³² Washington Times, "Iran's Twitter Revolution," <http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/>; and Zoe Fox, "How the Arab World Uses Facebook and Twitter," 6/8/2012, <http://mashable.com/2012/06/08/arab-world-facebook-twitter/>
- ¹³³ 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 <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/>
- ¹³⁴ <https://twitter.com/JeanBirnbaum/status/226348204160065537>
- ¹³⁵ NA, BIS Offers Enhanced Enforcement Plan For Items Subject To Reform Effort, Inside US Trade, 7/19/2012 <http://insidetrade.com/Inside-US-Trade/Inside-US-Trade-07/20/2012/bis-offers-enhanced-enforcement-plan-for-items-subject-to-reform-effort/menu-id-172.html>
- ¹³⁶ 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
- ¹³⁷ VOA, "The US Boosts Exports of Internet Services to Closed Societies," 3/10/2010, <https://www.youtube.com/watch?v=qLDIQzpd5kc>
- ¹³⁸ "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

¹³⁹ Amy Chozick, "Official Syrian Web Sites Hosted in the United States," 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>

¹⁴⁰ <http://www.state.gov/secretary/rm/2011/12/178511.htm>;
<http://www.state.gov/j/drl/rls/rm/2012/180958.htm>;

¹⁴¹ <http://geneva.usmission.gov/us-hrc/Internet-freedom-fellows-2012/>

¹⁴² <http://globalnetworkinitiative.org/>

¹⁴³ <http://Internetfreedomfund.tumblr.com/>

¹⁴⁴ <http://cordis.europa.eu/fp7/ict/fire/events/20120507-fire-nds-ws/ppts/01-no-disconnect-strategy-20120507-ag1.pdf>

¹⁴⁵ 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

¹⁴⁶ 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/>

¹⁴⁷ 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/

¹⁴⁸ 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.