Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy

BY DANIEL CASTRO AND ROBERT ATKINSON | SEPTEMBER 2014

The CompuServe case set off an international debate about the appropriateness of applying domestic laws to a global network—a debate which is even more heated, more important, and still unresolved to this day.

In 1995, Bavarian authorities raided the German offices of CompuServe and charged Felix Somm, the president of CompuServe's German subsidiary, with violating the law because the company did not block access to certain websites, including some sites containing child pornography and Nazi propaganda.[1] In response to these charges, CompuServe subsequently blocked access to two hundred online messaging boards for all four million of its customers worldwide, outraging many of its Internet users who were angry that German law could dictate what content was available to those outside its borders when other countries had more permissive laws about indecent and offensive content.[2]

In 1998, a German court convicted Somm and gave him a suspended two-year sentence and a fine, but the ruling was overturned a year later. This case set off an international debate about the appropriateness of applying domestic laws to a global network—a debate which is even more heated, more important, and still unresolved to this day.

The Internet is a global network that is fundamental to commerce, communication, and culture. The ability to use the Internet to purchase products and services from halfway around the world, to talk to friends and strangers in other countries, and to share and discover new ideas, is what has made the Internet the defining technology of the 21st century. But the same capabilities that make the Internet the incredible powerhouse that contributes trillions of dollars annually to the global economy—the ability to transfer data

seamlessly across geographic borders—has exacerbated the international conflicts that arise between nations with different laws and values.[3]

Even though the importance of the Internet to the global economy and society continues to grow each day, collectively nations have made little substantive progress in creating a framework for resolving the many conflicts over Internet policy that inevitably occur between sovereign nations. These conflicts arise over a myriad of issues, such as free speech, intellectual property, privacy, cybercrime, consumer protection, taxation, commerce regulation, and others. To date, despite many attempts, no framework has been successful at providing a practical and widely-accepted model for policymakers to resolve cross-border Internet policy conflicts in ways that respect both the global nature of the Internet and national laws and norms.

One reason for the lack of progress is that different nations have different sets of values and priorities, and attempts at resolving policy disputes inevitably falter because the various parties lack a common basis for dialogue. Another reason is that many proposed frameworks tend to apply a particular nation's worldview on the rest of the world, such as promoting democracy and freedom of expression (as in the case of the United States) or maintaining political control (as in the case of nations like China and Russia). But despite their appeal (e.g., they would be relatively easy to administer if everyone would just agree to one universal framework), such frameworks simply cannot work because nations have significantly different cultural values, policy priorities, and legal systems. It is highly unlikely Europe will agree to a U.S. privacy framework (or that the United States will agree to an EU privacy framework), or that Saudi Arabia will agree to U.S. free speech framework, especially when it comes to Internet pornography. But the alternative, a Balkanized, fragmented global Internet that gives nations the right to act on the Internet with impunity cannot be the answer either.

Collectively nations have made little substantive progress in creating a framework for resolving the many conflicts over Internet policy that inevitably occur between sovereign nations.

What is needed is a framework that allows nations the right to customize Internet policy to their own national needs and rules, while at the same time constraining those rights in ways that enable global Internet commerce and digital free trade while also preserving the underlying global Internet architecture, like the global domain name system. While nations will not always agree unanimously on specific policy proposals, appropriate solutions, or even the relevant evidence, a common framework of understanding cross-border Internet policy issues will allow for healthier Internet policy debates, better cooperation and coordination between nations, and fewer policy conflicts.

This report proceeds as follows: first, it explores the nature of cross-border Internet policy conflicts and provides a sample of the types of conflicts that have been seen in recent years; second, it discusses the limitations of existing Internet policy frameworks and offers an alternative perspective; third, it outlines a specific set of rules that should be used for evaluating cross-border Internet policy conflicts; and fourth, it operationalizes this framework using various examples to show the method in action.

WHY DO COUNTRIES HAVE CONFLICTS OVER INTERNET POLICY?

Internet policy determines the rules and structure of the Internet, from its basic technical architecture to the content distributed over the network. While some cyber-libertarians mistakenly believe the Internet is and should be a lawless land of virtual anarchy, the reality is that the Internet, like all other technologies and human practices, has always been guided by both formal and informal rules throughout its history.[4] These rules have been created at the sub-national, national, and international levels, by both governments and non-governmental organization alike. The result is an uncoordinated patchwork of laws, regulations, and standards created in a variety of forums.

Unsurprisingly, nations come into conflict with one another over Internet policy issues for a number of reasons. First, nations may disagree on the appropriate forum to address an issue. Policymaking occurs in many different forums at the sub-national, national and international levels. Conflicts occur, for example, when some nations want to address a certain policy issue domestically whereas others want to address it in an international forum. Conflicts may also occur within and between nations when policymaking at the subnational level is inconsistent with policy decisions made at the national level. For example, in the United States, certain states, such as California, sometimes create laws impacting the Internet that are not consistent with federal law. Conflicts also occur within nations, with some groups and interests arguing for one approach, and others arguing for a different approach. These conflicts can be magnified at the international level.

Alternatively, nations may agree to address an issue in an international forum, but disagree on which one. There are many different international forums for Internet policy. The Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) are non-governmental organizations for creating technical standards for the Internet and the World Wide Web, respectively, and the Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for creating the rules on how unique identifiers, such as domain names and IP addresses, are allocated and managed. The International Telecommunication Union (ITU) is an intergovernmental organization that develops international telecommunication regulations (ITRs) that address issues such as traffic flows and quality of service between telecommunication network operators, while the Organisation for Economic Co-operation and Development (OECD), the World Trade Organization (WTO), and the World Intellectual Property Organization (WIPO) are intergovernmental organizations also involved in cross-border agreements that may affect Internet policy issues. Many nations have also signed regional trade agreements that include Internet policy matters in them. Other organizations involved in Internet policy include the Internet Society, the Internet Governance Forum (IGF), Internet Research Task Force (IRTF), the Regional Internet Registries (RIRs), and the International Organization for Standardization (ISO). Each of these organizations has its own set of rules and processes. Conflicts also sometimes occur when countries agree on a forum, but disagree on the rules in place or how those rules are created.

Second, nations may disagree over questions of jurisdiction. The inherently cross-border nature of the Internet means that nations are often at odds with one another over who has jurisdiction over a particular Internet policy issue and whose rules, if any, will apply. In

addition, the rules that one nation adopts may impact those outside its borders. While no nation is willing to cede its legal authority to address actions either originating from or impacting those within its geographic borders, there are practical limits to what individual countries can do. For example, a nation might very well pass a law criminalizing certain activities on the Internet, but if these activities occur outside of its borders and it has no direct authority over the individuals or organizations involved, it may have little luck enforcing such laws without international cooperation.

Moreover, when there are disagreements over jurisdiction, individuals and organizations may be caught between conflicting laws. Even though the Internet is global, no organization can realistically be expected to comply with the laws of every country in the world simply because they are on the Internet and some of their users might be based in another country. The costs of monitoring so many legal requirements, in addition to the costs of actually complying with them, would be prohibitive. And in some cases, the laws may be conflicting in such a way that it is simply impossible to be in compliance with all of them. Neither can organizations be expected to routinely show up to defend themselves in foreign courts when they have never set foot in that country before.

Even though the Internet is global, no organization can realistically be expected to comply with the laws of every country in the world simply because they are on the Internet and some of their users might be based in another country.

Conflicts over jurisdiction can be difficult to resolve. For example, if a hacker in China breaks into a French company's server located in Brazil and steals data from the company's Canadian users, which country's laws apply? And what recourses do nations have if other nations do not take action to prevent a crime or disagree that a crime has taken place? Multiple criteria are used by courts to determine when a country has the authority to impose its laws on those outside of its borders. When determining whether a country has jurisdiction over an organization, factors such as physical presence, business activity, and marketing will likely be considered. For example, if a firm based exclusively in China creates a children's mobile app that is popular in China, but it does not advertise this app in the United States, it will likely not have to comply with the Children's Online Privacy Protection Act (COPPA), a U.S. law which regulates privacy, because in practice authorities in one country often have little ability to exert control over firms in another nation.[5]

Jurisdictional conflicts on the Internet should be resolved by considering an analogy to the physical world. If a Chinese firm attempts to export a product to the United States, its product can be blocked by U.S. officials if it is not in compliance with consumer product safety law. But if U.S. citizens travel to China to purchase the product, then the Chinese firm does not have to comply with U.S. laws (although U.S. citizens must still comply with U.S. laws and may be prevented from returning to the United States with the product). The same analogy should be extended to Internet commerce. If a Chinese Internet firm exports its content or services to the United States by, for example, advertising its services in the United States or setting up a U.S. office, then it should be subject to U.S. law, just as a Chinese exporter would be subject to U.S. law. But if a U.S. citizen goes to a Chinese website, that website should not be expected to have to comply with U.S. law, any more than a Chinese firm would be expected to comply with U.S. law because it was selling to U.S. tourists visiting China on vacation.

However, some policymakers believe that their national sovereignty gives them the right to dictate policy for the entire Internet since it crosses their country's borders. To continue with the consumer product analogy, some nations might say that since their citizens might travel to a foreign nation and buy a product that is not in compliance with their consumer product safety laws, then these foreign nations should be required to adopt the domestic country regulation. When applied to the Internet, this notion has been particularly distressing to Internet users in Western countries who fear that government-led policymaking on the Internet will pervert the openness and freedom that characterized the Internet's earliest years (although many of these same users also oppose efforts by their own governments to regulate activity on the Internet).

Third, countries may disagree over the extent to which a policy issue should be addressed by nation states versus non-state actors. While the development of the Internet stemmed from a U.S. government-funded project, and to this day the U.S. government has retained supervisory authority over certain technical features of the Internet (at least indirectly, through its contract with ICANN), Internet users have been largely responsible for setting the rules governing the Internet architecture itself. As the number and diversity of Internet users has increased, conflicts have arisen not only because different stakeholders have different values, but also because national governments have tried to have a greater role in setting policy about how the Internet is used.

Fourth, nations often disagree over specific policy goals or measures. At the national level, rules about the Internet are determined by legislators, regulators and courts. For example, in the United States, Congress decides issues about taxing Internet access, the Federal Trade Commission regulates unfair or deceptive commercial activities, including online advertising, and the Federal Communications Commission sets the rules for allocating spectrum among network operators. In the United Kingdom, the Information Commissioner's Office (ICO) issues guidance on how websites should safeguard user privacy.[6] In China, the Ministry of Public Security runs the Golden Shield program (commonly referred to as the "Great Firewall of China") which restricts access to certain websites and services.[7] Rules set at the national level may conflict with other nations either directly or indirectly. These disagreements may stem from different values or priorities, such as a preference for protecting free speech over preventing hate speech. Alternatively, nations may disagree over specific policies because the costs and benefits are distributed unevenly between nations, as is the case when nations turn a blind eye to online piracy in order to allow their citizens to gain access to foreign copyrighted materials without paying.

Internet policy is a wide-ranging field covering a significant variety of different issues. Some of these issues, such as intellectual property, often result in a nation creating domestic policies that have an impact on those outside its borders, while others, such as Internet access, are mostly limited to domestic policy. Many Internet policy issues fall into a specific category while others span multiple categories. The following list of categories is not meant to be exhaustive; rather, it reflects the diversity of issues that fall under the rubric of Internet policy.

The categories of Internet policy issues include:

- Content regulation (e.g., freedom of expression, censorship, decency, hate speech, libel, etc.);
- Intellectual property (e.g., copyright, patents, trademarks, etc.);
- Data (e.g., privacy, security, data residency, mutual legal assistance treaties, etc.);
- Commerce (e.g., e-commerce regulation; gambling regulations; taxes; trade policy; consumer protection; anti-trust and competition; sales of regulated goods, such as pharmaceuticals and tobacco; and sales of contraband, etc.);
- Cybercrime (e.g., spam, malware, fraud, denial of service, intrusions, botnets, cyber stalking, harassment, etc.);
- Network operation (e.g., spectrum allocation, IP address allocation, domain name allocation, interconnection agreements, international telecommunication regulations, etc.);
- Network performance (e.g., protocol standards, network security, network design, conformance testing, etc.); and
- Equity and access (e.g., broadband subsidies, digital literacy, connected schools and communities, computer ownership, etc.).

Most nations (as well as sub-national entities) at least consider policy proposals in all of these categories, and they often come into conflict with each other when the objectives of two countries are not aligned or when the impact of a specific proposal has negative consequences for others. For example, conflicts may arise over divergent goals for surveillance and privacy or censorship and free speech. Table 1 provides a brief snapshot of the types of decisions made about Internet policy in recent years. As the table shows, there are potential cross-border conflicts over almost every aspect of Internet policy.

Type of Issue	Examples
Content regulation	In 2013, the Vietnamese government issued a decree to restrict individuals from sharing certain types of information, potentially including news articles critical of the government, on social media.[8] In 2013, at the behest of the government, British Internet service providers (ISPs) agreed to enable parental filtering for pornographic materials by default, while allowing users to request their ISPs to disable this option.[9]
Intellectual property	In 2011, the Swiss government decided to refrain from pursuing legislation that would criminalize illegal downloading of copyrighted content such as music and movies, and instead allow individuals to have a legal right to download infringing content for personal use.[10] In 2009, France passed a law to create a state agency tasked with warning Internet users suspected of illegal file sharing. If users ignored the warning, their case could be referred to a court where the users might be fined, or eventually, have their Internet access suspended. The policy was halted in 2013.[11]

Data	In 2013, Brazilian President Dilma Rousseff proposed legislation that would require foreign Internet companies to store their data in data centers located in Brazil.[12] In 2012, a Spanish citizen filed a complaint with the Spanish Data Protect Agency (AEPD) because a newspaper contained information about the auction of real estate property seized from him for "non-payment of social security contributions." The AEPD ordered Google to eliminate 100 links about the individual from future search results.[13]
Commerce	In 2013, the French government began lobbying the European Union to modify corporate tax rules so that Internet companies would pay taxes based on the location where revenue is generated.[14] In 2010, the Australian Government banned advertising tobacco products on the Internet.[15]
Cybercrime	In 2013, the U.S. Federal Bureau of Investigation (FBI) hacked into the French servers of an Irish organization alleged to be providing web hosting for criminal purposes, such as distributing child pornography. The FBI then installed malware on these servers so that anonymous Internet users accessing content on these servers could be identified by law enforcement.[16] In 2013, the EU parliament's civil liberties committee approved draft legislation to establish minimum prison sentences for hackers.[17]
Network economics	In 2012, Russia proposed that the International Telecommunication Union (ITU) update the International Telecommunication Regulations (ITRs) so that authority to allocate IP addresses would be reassigned from ICANN to the ITU.[18] In 2011, the U.S. government sought to have ICANN grant veto authority to countries over proposed top-level domains. ICANN demurred and instead granted countries the ability to offer non-binding recommendations.[19]
Network performance	In 2012, India's Department of Electronics and Information Technology issued an order requiring computers and other electronics to undergo conformance testing at domestic labs using standards that deviate from global norms.[20] In 2011, representatives of China, Italy and France voted for the International Telecommunication Union Standardization Sector (ITU-T) to adopt a particular networking standard favorable to their domestic hardware manufacturers, but that was incompatible with the existing standard developed in the Internet Engineering Task Force (IETF).[21]

Table 1: Recent examples of Internet policy decisions and conflicts

WHY DO EXISTING FRAMEWORKS DO A POOR JOB IN RESOLVING CROSS-BORDER INTERNET POLICY CONFLICTS?

Resolving the myriad and growing number of cross-border Internet policy conflicts is difficult. But it would be easier if nations could adopt a framework that laid out principles for policy resolution. At this time there are two dominant approaches to cross-border Internet policy, neither of which provides meaningful solutions for handling the complexities of competing international priorities and jurisdictions.

The first approach to resolving cross-border Internet policy conflicts can be termed "universalism," or an attempt to apply the same set of rules to all countries. If everyone buys into the same rules and norms, they minimize conflict. While universalism can manifest itself as the view that all nations should strictly control the Internet, such as by limiting online freedom and Internet openness, in practice the most fervent calls for universalism have come from cyber-libertarians in the West with calls for universal rules such as "Internet freedom for all," "no online censorship," "information wants to be free," and "all Internet packets should be treated the same."[22] While these types of universal rules appeal to the perspective of certain individuals in some democratic nations like the United States, by no means do all nations share this view, including, but not limited to, those run by authoritarian governments.

Universal rules make sense in certain situations, but in many cases they are inappropriate for Internet policy because countries differ too much in their values and priorities.

To be sure, universal rules make sense in certain situations (e.g., rules on responding to denial of service attacks, frameworks on core Internet architecture, agreements regarding digital trade, etc.), but in many cases universal rules are inappropriate for Internet policy because countries differ too much in their values and priorities. For example, countries vary widely in their treatment of hate speech, even democratic ones. France and Germany have strong laws combatting anti-Semitism and other forms of non-violent hate speech, whereas the United States puts a premium on free speech rights. Attempting to reconcile these conflicting laws to create universal rules for regulating speech on the Internet is futile and doomed from the start. Likewise, democratic nations have very different approaches to Internet privacy, with many in Europe seeing privacy as a fundamental human right while many in the United States see privacy as just one value to be considered among many (e.g., innovation and economic growth).

One particular strain of universalism is cyber-libertarianism, whose advocates call for government to keep its hands off the Internet. In effect, cyber-libertarians want one universal rule: "no government-imposed rules." John Perry Barlow's "Declaration of Independence from Cyberspace" is the epitome of the cyber-libertarian philosophy, in which he states that national governments have no authority on the Internet and are unwelcome.[23] Even more so than other attempts at universalism, this worldview is neither practical nor reasonable; attempts to advocate a hands-off approach to Internet policy will consistently run into objections by policymakers who identify legitimate (and in some cases illegitimate) government interests. For example, many would agree that governments have a legitimate role to play in protecting consumers from unsafe, counterfeit drugs that are sold online.

Various other advocates have offered their own frameworks for universal rules for the Internet. For example, former U.S. Secretary of State Hillary Clinton's influential "Internet Freedom" speech in 2010 outlines the "Internet Freedom" agenda, which describes unfiltered Internet access as a fundamental human freedom and tool for advancing human rights and democracy and calls for all nations to embrace the open Internet.[24] World Wide Web creator Tim Berners-Lee has similarly called for a "Magna Carta" for the Internet to create universal rights for privacy and free speech online, both values Berners-Lee endorses.[25] Other popular views include those advocated by notable figures such as Julian Assange, the founder of Wikileaks, whose manifesto describes the Internet as a force for creating transparency in government and ending corruption, and Jimmy Wales, the founder of Wikipedia, who describes the Internet as a force for knowledge and fighting censorship.[26]

In the past few years, different groups have continued to release new sets of principles, frameworks or guidelines for Internet policy that focus on universalist paradigms. These include:

- "Communiqué on Principles for Internet Policy-Making," a framework from the Organisation for Economic Co-operation and Development (OECD) on how to create a more transparent and open Internet;[27]
- "Toward A Single Global Digital Economy," a report from the Aspen Institute's International Digital Economy Accords (IDEA) project promoting market access, the free flow of information, and a trusted environment on the Internet;[28]
- A "Code of Conduct for Government Leaders" from the World Economic Forum's Global Agenda Council on Informed Societies calling for more open societies and the spread of information;[29]
- The Global Network Initiative charter, which advocates advancing freedom of expression and privacy online;[30]
- The European Union-United States "Trade Principles for Information and Communication Technology Services," which outlines a set of principles to promote economic development;[31]
- "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," a report from the White House outlining a framework for developing privacy protections for consumers; and
- The European Commission proposal to reform data protection and privacy rights.[32]

There is nothing wrong with these frameworks. On the contrary, many of them are commendable and represent thoughtful recommendations for policymakers either about Internet governance broadly or a specific issue. In addition, they may also be useful for advocacy groups and diplomats in promoting their respective agendas, whether it is the

spread of democracy or the rights of disadvantaged populations. But since these views are espoused by individuals, groups or organizations with the aim of achieving a specific policy outcome—such as the spread of democracy, the promotion of privacy, or the full expression of individuals—and these outcomes are not necessarily universally shared by all stakeholders in the Internet ecosystem, they cannot serve as a useful starting point for debating Internet policy issues for those who do not share the same goals. For example, while many in the United States would oppose any attempts by the government to censor online pornography, many others in countries around the world find the content deeply offensive and would prefer to ban it (just as many in the United States have tried to ban pornography). While there is nothing wrong with the U.S. government and related civil society groups advocating for U.S. values around the world, they should not expect that their values can or should constitute a global approach to Internet governance.

A second approach to Internet policy is to take the complete opposite perspective and advocate for each country to have near complete freedom to do what it wants. In many ways, this is the dominant approach to Internet policy today where countries sometimes engage in conflict over a policy but ultimately each country goes its own way. The problem is that the policy decisions of one country can sometimes create significant negative externalities for individuals and businesses outside of that country which are likely not taken into consideration. Or a nation may pass a law that impacts those outside of its jurisdiction and is simply unenforceable.

While there is nothing wrong with the U.S. government and related civil society groups advocating for U.S. values around the world, they should not expect that their values can or should constitute a global approach to Internet governance.

There are three main drawbacks to the current approach. The first is that it leads to Balkanization of the Internet—instead of a single, global Internet, each country pursues its own "national internet" with its own set of rules. Balkanization erodes the universality and efficiency that comes from a fully interconnected global network, which is one of the main benefits of the Internet. Indeed, if Balkanization extends beyond policy and to the Internet architecture itself, it could erode the worldwide nature of the Internet. The second drawback is that it can lead to one nation's values and laws being imposed upon others without the other nations affirmatively choosing those values or laws for themselves. The third is that these policies can be used as cover for what are essentially anti-competitive, trade-distorting actions that hurt the global economy.

AN ALTERNATIVE APPROACH TO CROSS-BORDER INTERNET POLICY

While both approaches—universalism and Balkanism—have problems, they are not without their merits. Universalism appeals to the desire to have cooperation between different nations, while Balkanization minimizes many of the problems associated with conflicting policies. Combining both of these frameworks yields an alternative approach to Internet policy that captures the best of each approach while sidestepping their pitfalls.

The first step is to recognize that when it comes to the Internet's technical architecture, a universalist approach to promulgate global, commonly shared standards is necessary. Countries that wish to participate in the Internet must agree on a common technical architecture (e.g., domain names, networking protocols, etc.), otherwise it would degenerate into a series of national-level networks. A multi-stakeholder approach to maintaining this goal is desirable since debates and disagreements over the technical

architecture of the Internet can only be resolved if stakeholders reach consensus. And the Internet, which is a network of networks, has vastly more stakeholders than previous telecommunications systems, such as the telephone system, where in most nations the state was the owner. Although countries have not signed binding international agreements committing to the multi-stakeholder approach for the continued development of the Internet, doing so would be a useful way to codify this model, particularly in light of the transition away from U.S. oversight of ICANN.[33]

The second step is to recognize that when it comes to policies about the how the Internet is used, as opposed to policies about how the Internet is constructed or how it operates (e.g., Internet architecture), there can be differences between nations. Ideally, international agreements would allow nations to achieve and formalize consensus on various policy goals, particularly those that have an effect on individuals outside the country. These agreements would allow nations to specify goals that are both desirable (universal "goods") and undesirable (universal "bads") from a global perspective. In general, nations should oppose policies that interfere with or limit universal "goods" and support policies that interfere with or limit universal "bads". For example, the existence of the WTO is evidence of broad international consensus on the benefits of free trade (a universal "good"). Thus WTO members should support Internet policies that promote free trade in digital goods and services and actively oppose those that conflict with it. Similarly, as there is broad international agreement on the need to combat child pornography (a universal "bad"), including a UN human rights treaty, signatory nations should support Internet policies designed to reduce this criminal activity.[34]

Although countries have not signed binding international agreements committing to the multi-stakeholder approach for the continued development of the Internet, doing so would be a useful way to codify this model, particularly in light of the transition away from U.S. oversight of ICANN.

In the former case, these nations should use related processes to address cross-border Internet policy conflicts that are inherently about trade. To do so, they might turn to the WTO to address Internet policy conflicts principally focused on trade to constrain nations that attempt to limit digital trade (a universal "good"). In contrast, nations that have signed global agreements to limit universal "bads" would be within their rights to require Internet actors in their nation to change their actions according to the rules, even if they affected users outside that nation.

However, where there is no consensus on the broad goal, nations should limit their policymaking activities to proposals that do not impact those outside their borders. For example, if a nation wants to impose a special tax on certain online services (a "local good"), and these taxes are not violating any international agreements, it should be allowed to do so domestically.[35] Or if a nation wants to prevent access to online pornography and this activity is not covered by an existing international treaty (a "local bad"), then it should be allowed to do so as long as its methods do not significantly affect users in other countries. Thus if a country blocks access to certain sites deemed offensive domestically, such that the blocking does not affect users outside of its borders, other nations should not interfere, unless such reasons are in fact a pretense for limiting a universal good (e.g., international trade).

As shown in Figure 1, the left side of the table (i.e., universal goods and universal bads) represents the opportunity for universalism. Nations should work to develop formal

international agreements where there is consensus on policy goals but no existing bi-lateral or multi-lateral agreements. For example, since most nations agree on the need to increase the reliability of the network, combat spam, and deter cybercrime, these are areas of ripe opportunity to develop international agreements.

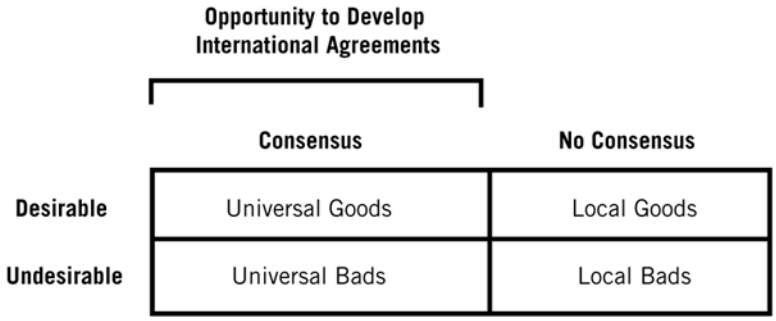


Figure 1: Typology of Internet policy goals affecting individuals outside the country

Where they do not have consensus (i.e., local goods and local bads), nations should be allowed to go their own way, so long as the impact of their policies has a limited external impact.

HOW POLICYMAKERS CAN OPERATIONALIZE THIS FRAMEWORK

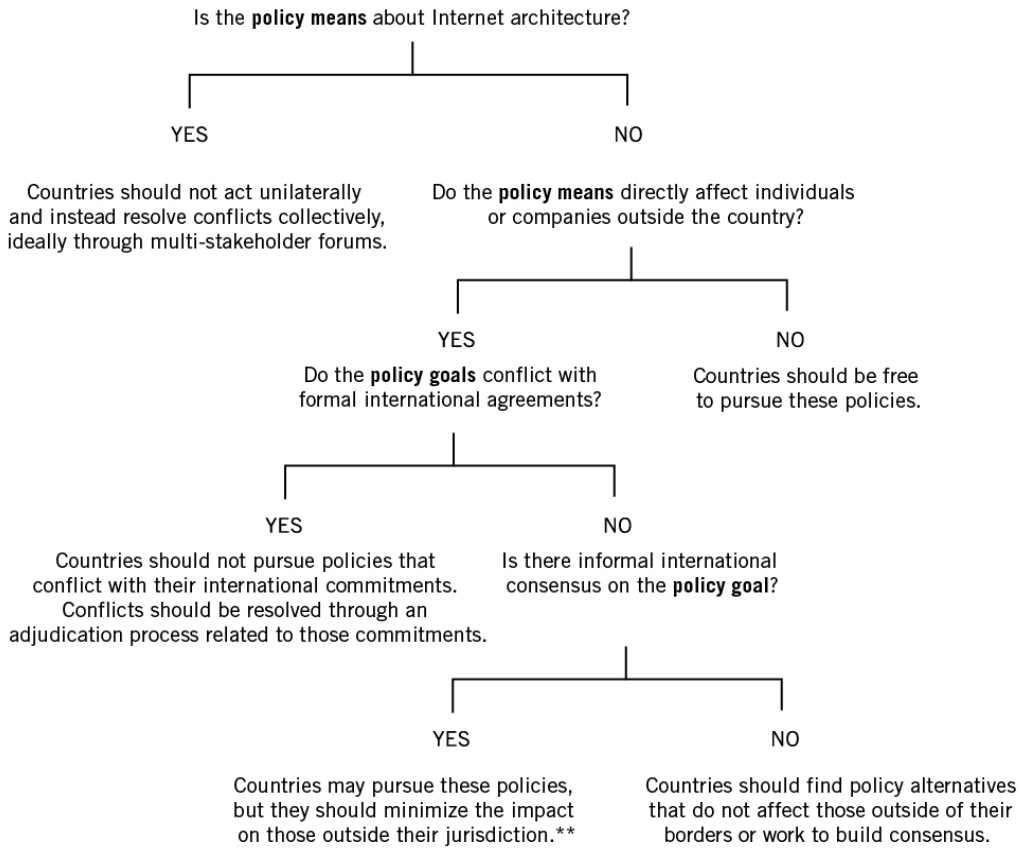
Policymakers around the world can use this framework to decide how to respond to Internet policy conflicts. The framework is indifferent to the particular policy issue, and instead is based on whether the issue affects the core Internet architecture or the use of the Internet, and whether there is international consensus on policy objectives and the degree to which domestic policies affect those outside a nation's borders.

As Figure 2 illustrates, policymakers must consider both the ends and means of a particular policy. The first question is whether the policy will affect Internet architecture. If it does, countries should not act unilaterally and instead should work to resolve the issue, ideally in a multi-stakeholder forum.

If it is not about Internet architecture (which, as we discussed above, should be inviolate and international in its nature), but is instead about the use of the Internet, then the next consideration is whether the method by which the policy will be implemented will directly affect those outside the country. If there is no direct impact on individuals or businesses in other countries, then a country should be free to pursue these policies (i.e., there is little or no cross-border policy conflict). This is not to say that certain countries need to endorse the policies of other countries, or even that they cannot try to dissuade them from pursuing a course they disagree with. Rather it is to say that ultimately these are issues where different countries should be allowed to "agree to disagree." For example, Western democratic nations may not like the fact that the Chinese government blocks access to online political content it deems threatening, but fundamentally that is its right as a sovereign government. In contrast, as a signatory of the WTO, China likely does not have

the right to keep foreign competitors from selling products and services online to its residents.

On the other hand, if the policy means will have an impact on individuals outside of a country's borders, then additional questions need to be considered. The next question is: do the policy goals conflict with a nation's existing international agreements, such as free trade agreements or other international treaties? If there is a conflict, then the policy should not be pursued. Countries should be held to their commitments, and therefore should not enact policies that conflict with formal international agreements. Naturally, countries may disagree about whether a proposed policy presents a conflict with an international agreement. For example, one country might argue that a policy is a trade agreement violation whereas another might argue it isn't. These disputes must be resolved in an appropriate forum, such as the WTO for digital trade disputes. If such a forum does not exist for a particular issue, then countries should work to develop an appropriate forum for adjudicating whether a policy is in conflict with an international agreement.



** Policy makers should focus on developing international agreements to solutions for these problems.

Figure 2: How to Evaluate Internet Policies

If the policy goal does not conflict with international agreements, then the final question to ask is whether an informal consensus exists among countries that a certain policy objective is desirable. Informal consensus may be reflected in non-binding international charters, or in cases where many countries have similar domestic laws. If there is informal consensus on the policy goal, then countries may pursue the policy, but they should do so cautiously and seek to minimize the impact on those outside of their jurisdiction. These areas of informal consensus are ripe opportunities for policymakers to focus on developing binding international agreements since many countries are already in agreement on broad principles and others may be interested in committing to solutions that do not negatively impact their peers. For example, since most countries have laws designed to combat cyber-attacks, there are likely areas where countries may be able to work closer together, such as to standardize how law enforcement officials request and gain access to digital records as part of a criminal investigation.

If there is no informal consensus on the policy goal (e.g., protecting hate speech), then countries should find policy alternatives that do not affect those outside of their borders or work to build consensus on the particular policy objective. A country that pursues policies affecting those outside its borders where there is no international consensus on the goal should work to find an alternative that minimizes the impact outside of its borders. Absent that, the country should face global pressure to rescind its actions.

A country that pursues policies affecting those outside its borders where there is no international consensus on the goal should work to find an alternative that minimizes the impact outside of its borders.

THIS INTERNATIONAL INTERNET POLICY FRAMEWORK IN ACTION

Various examples illustrate how this framework can be used. The following examples consider each of the four potential outcomes from the framework.

Case #1: Thailand Passes Internet Censorship Legislation

In 2007, Thailand passed the Computer Crime Act, which, among other things, allowed the government to obtain court orders to block content on the Internet. Between 2007 and 2011, the government blocked over 80,000 URLs, the majority (75 percent) for content considered insulting or defamatory to the Thai monarchy and almost all of the rest (24 percent) for pornographic content.[36] Websites hosted within the country were expected to remove the content, but websites outside of the country were not. Instead, Internet service providers (ISPs) blocked these foreign websites.

In this case, the policy goal was to limit access to offensive content. Thailand used two policy means to pursue this goal. First, domestic websites were asked to remove the offending content. Since this content can be reposted on foreign websites, this policy has a negligible effect on those outside the country. While some countries may question the policy's efficacy and its alignment with Western ideals of democratic freedom, this policy falls into the category of policies where countries should acknowledge their different values and move on.

The second policy means was to have domestic ISPs block users from accessing offensive foreign websites. This policy does have an effect on individuals and companies outside the country since they cannot communicate with or sell their services to domestic users. In addition, because of network effects—where the value of a good or service increases with

the number of users—blocking access to such sites may also have an incremental effect on the value of some online services for users outside the country. Using the framework, we should next consider whether the policy goal conflicts with international agreements. It does not appear that a broad coalition of countries have signed binding international agreements either banning (or permitting) this type of content. Since the policy goal does not conflict with international agreements (i.e., it does not appear to be backdoor method to trade protection), we should then consider whether there is informal international consensus on the policy goal. In fact, most countries do have some laws outlawing certain types of content deemed to be offensive. So using the framework, Thailand should be free to pursue policies along these lines since they made an effort to minimize the impact on those outside their jurisdiction (i.e., foreign users can still access the restricted content). In this case, the motivation for the policy appears clearly related to social and cultural issues, rather than protectionist measures to defend Thai content creators.

Case #2: France Proposes Law Limiting Discounts for Online Book Sales

In 2013, French lawmakers proposed a bill that would prevent online retailers from offering free shipping on discounted books.[37] France already regulates the prices of books sold in brick-and-mortar stores, and this law is intended to modernize this regulation for e-commerce. Since 1981, French law prohibits bookstores from selling books for less than 5 percent below the cover price. The intent of this law is to protect small, independent book sellers from large retail chains that have economies of scale that let them provide discounts to French consumers. French policymakers see preserving independent bookstores as an important part of France's cultural identity, even if French consumers pay a price in the form of higher book prices. In contrast, the norm in countries like the United States is to maximize consumer welfare (e.g., lower prices for consumers), not producer welfare (e.g., higher profits for small bookstores). As it is written, the law applies to all online retailers, although Amazon, a U.S.-based Internet company, would be significantly impacted by the law.

In this case, the proposed law would directly affect both domestic and foreign companies (although only foreign companies doing business in France). The next question to ask is whether the policy goal conflicts with international agreements. Here there might be some dispute. On the one hand, some might argue that this law is anti-competitive and violates free trade agreements to which France is a signatory. Indeed, French lawmakers acknowledge the law was intended to target online retailers such as Amazon that were undercutting the price of French booksellers. If that is the case, then France may be in violation of trade agreements and the United States may consider filing a complaint with the WTO.

On the other hand, this law would apply equally to both foreign and domestic companies who do business in the country, and so the fact that Amazon might be disproportionately affected may only be incidental. Arguably the French government is consistent in trying to protect independent book sellers from both online and offline competition. The policy goal in this case is preserving culture, a policy goal that is not in conflict with international agreements and has broad international support. Thus if the WTO were to rule that France is within its rights here, other countries should accept that France has authority to pursue

this policy, in part because it would not affect foreign companies outside of the jurisdiction of French law (i.e., it only affects companies directly selling to French citizens). Again, other countries might very well point out that this is a bad law that will result is higher prices for consumers and less convenience for French consumers, but ultimately concede that France should be allowed to do as it pleases in this regard. Alternatively, if a country believed the policy goal was not preserving culture, but rather preventing legitimate foreign trade, it should bring a trade dispute to the WTO and resolve the issue in that forum.

Case #3: United States Blocks Foreign Internet Gambling Websites

In 2006, the United States enacted the "Unlawful Internet Gambling Enforcement Act," which restricted banks and credit card companies from sending funds to off-shore Internet gambling websites. Although the United States has outlawed much of Internet gambling domestically, it has provided some exceptions for domestic online betting on horse races.[38] Countries that are home to major online casinos, such as Antigua and Barbuda, have seen a major loss of revenue as U.S. consumers could not complete transactions with their websites.

In this case, foreign businesses were directly affected by the U.S. policy. If the policy goal was only to regulate online gambling, and there were not any binding international agreements relating to online gambling, then the United States would not be in violation of its commitments and should be free to pursue this policy as long as it minimized the impact on those outside of its jurisdiction (i.e., as long as its policy did not limit the operation's foreign online gambling).[39] However, if one of the goals of the law is to impose trade restrictions on other nations in violation of its trade agreements, then the United States should modify its policy. In this case, Antigua and Barbuda raised objections to the World Trade Organization, and the WTO ruled against the United States. The WTO found that the United States failed to fulfill its commitment to grant others "full market access in gambling and betting services."[40] Whether or not the United States agrees with the WTO ruling, given that it is a signatory to the WTO agreement, the United States should modify its laws to come into compliance.

Case #4: China Prohibits Anonymous Internet Access

In 2012, China passed a law prohibiting Chinese residents from purchasing Internet access anonymously.[41] Although the Chinese government already closely monitors Internet activity, the new law would require Internet users in China to register with their real names when signing up for service.[42] In this case, the policy means has little to no effect on individuals and businesses outside of China, so countries should recognize the Chinese government's authority to impose these rules. Again, this is not to say that other countries could not continue to lobby foreign governments to create policies in line with their own values or promote the potential benefits to political speech of anonymity on the Internet, but only that a policy like this need not be part of cross-border Internet policy conflicts. In contrast, China's continued policy of not restricting online copyright infringement has a clear effect beyond its borders on the welfare of rights holders and represents a legitimate cross-border Internet policy conflict.

Case #5: Singapore Law Gives Copyright Owners Ability to Request ISPs Block Access to Infringing Content

In 2014, Singapore passed an amendment to its Copyright Act which would allow rights holders to go to court and obtain an injunction to have ISPs block access to websites containing flagrantly infringing content, even those hosted outside of Singapore.[43] Website owners can apply to have the block revoked if they remove the infringing content. Since foreign users would still be able to access the blocked website, this would have a minimal effect on those outside the country. Therefore, since the direct impact is limited to domestic users, Singapore should be free to pursue this policy. This type of blocking would also not be a violation of free trade, as the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement generally allows countries to offer copyright protections.[44]

Case #6: Italy Privacy Law Holds Executives Responsible for Third-Party Content

In 2010, a court in Milan found three Google executives guilty of Italian privacy laws for allowing a video to be posted online to Google Video—a predecessor to YouTube that allows users to share videos online—showing a disabled student being bullied. Each executive was sentenced to six months of jail after the prosecutor convinced the court that websites are responsible under Italian law for prescreening content before it is posted and obtaining consent of those depicted, even though prescreening every user-submitted video would significantly raise the cost of providing this free service.[45] None of these Google executives were in Italy for the prosecution of this case.

In this case, the policy means is a criminal statute applied to both individuals within the country and those outside of it, so clearly the policy affects those outside the country's borders. The next question is whether the policy goals align with international agreements. There are no binding international agreements relating to online privacy, obtaining consent for content posted online, or liability for online intermediaries. Neither is there informal consensus for these policy goals as various countries have widely different laws in this regard. As such, the framework notes that Italy should find a policy alternative that does not affect those outside its borders, or else build consensus internationally for its policy goal. For example, it could pass a domestic law making it illegal for its own citizens and residents to upload content depicting children being bullied.

Case #7: China Proposes Technical Standard to Partition Internet

In 2012, a group of three Chinese engineers, including one from China Telecom and one from China Mobile, the largest fixed-line and mobile state-owned telecommunications companies in China, respectively, proposed a new standard that would realign the domain name system (DNS) along national boundaries.[46] Rather than having a universal name space based on a single root, users would signal if they were trying to reach a domain on an alternative root. Countries would establish a peering system so that addresses could be translated between different systems.[47]

Using the framework, the first question to ask is whether the proposed policy is about Internet architecture, and in this case, it clearly is. Since this proposal is being made in the IETF, a multi-stakeholder forum, China is operating appropriately. Within this forum, other stakeholders can discuss the pros and cons of such a proposal, refine it if necessary,

and then choose whether it merits adoption.[48] Their choice should dictate the resulting policy.

CONCLUSION

To date, global Internet policy has vacillated between the poles of universalism and Balkanism. Universalists—whether advancing an open or closed vision of the Internet—see any efforts that accept anything less than universal rules as abandoning the struggle for the "right" approach. But the United States should take a page out of Cold War history, and in particular George Kennan's strategy of containment of the communist threat. Kennan was not accepting communism when he advocated to U.S. leaders that they try to contain the spread of communism until it died its own natural death, rather than pursue the risky strategy of trying to roll it back. Rather he was being a realist. Likewise, while the U.S. government should advocate for global values such as human rights and free speech both online or offline, the government should recognize that this cannot be the basis of our actual negotiations when it enters into forums like the ITU or ICANN. There, pragmatism and attempting to implement the framework laid out here should be the goal.

Collaboration is necessary to address many challenges on the Internet, from settings standards to preventing digital crime, and cooperation and coordination is required for countries to share in the benefits of the global network economy.

Indeed, the framework proposed here is conceptually simple. Many of the conflicts between nations in Internet policy come about because of different goals or values. For example, some countries may be concerned with eliminating the spread of hate speech, while others are more interested in protecting free speech. Or some countries may consider that access to information trumps privacy, while others prefer the reverse.[49] Yet even though all nations may not agree on the same goals or values, that does not mean they cannot work together to build a global Internet system that works well. Indeed, collaboration is necessary to address many challenges on the Internet, from setting standards to preventing digital crime, and cooperation and coordination is required for countries to share in the benefits of the global network economy. By using a common framework for analyzing cross-border Internet policy issues, and understanding which issues should be contested and which should not, policymakers can avoid unnecessary conflicts and better identify the validity of criticism of different Internet policy proposals.

ENDNOTES

1 "CompuServe Charged Under Anti-Porn Law," *Los Angeles Times*, April 17, 1997, http://articles.latimes.com/1997-04-17/business/fi-49523_1_compuserve-charged-german.

2 "Europe Ex-CompuServe boss acquitted," *BBC News*, November 17, 1999, http://news.bbc.co.uk/2/hi/europe/524951.stm.

3 Robert D. Atkinson et al., "The Internet Economy 25 Years After .com" (ITIF, March 15, 2010), http://www.itif.org/files/2010-25-years.pdf; James Manyika and Charles Roxburgh, "The great transformer: The impact of the Internet on economic growth and prosperity" (McKinsey Global Institute, October 2011), http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_great_transformer.

4 Daniel Castro, "A Declaration of the Interdependence of Cyberspace," *ComputerWorld*, February 8, 2013, http://www.computerworld.com/s/article/9236603/A_Declaration_of_the_Interdependence_of_Cyberspace?pageNumber=1.

5 Federal Trade Commission, "FTC Sends Educational Letters to Businesses to Help Them Prepare for COPPA Update," news release, May 15, 2013, http://www.ftc.gov/news-events/press-releases/2013/05/ftc-sends-educational-letters-businesses-help-them-prepare-coppa; Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions," accessed April 2014, http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions.

6 The Federal Communications Commission website, accessed July 8, 2014, http://www.fcc.gov. See also: the Information Commissioner's Office website, accessed July 8, 2014, http://www.ico.org.uk/.

7 George Chen, "China to lift ban on Facebook – but only within Shanghai free-trade zone," *South China Morning Post*, September 24, 2013, http://www.scmp.com/news/china/article/1316598/exclusive-china-lift-ban-facebook-only-within-shanghai-free-trade-zone.

8 Gerry Mullany, "U.S. Denounces Vietnam's New Limits on Dissent on Internet," *New York Times*, August 6, 2013, http://www.nytimes.com/2013/08/07/world/asia/us-assails-new-limits-on-internet-in-vietnam.html?ref=technology.

9 Kadhim Shubber, "ISPs to include porn filters as standard in UK by 2014," *Wired UK*, June 14, 2013, http://www.wired.co.uk/news/archive/2013-06/14/parental-filtering-industry-standard.

10 "Swiss Govt: Downloading Movies and Music Will Stay Legal," *TorrentFreak*, December 2, 2011, http://torrentfreak.com/swiss-govt-downloading-movies-and-music-will-stay-legal-111202/.

11 "France ends three-strikes internet piracy ban policy," *BBC News*, July 10, 2013, http://www.bbc.co.uk/news/technology-23252515.

12 Brian Winter, "Brazil's Rousseff targets internet companies after NSA spying," *Reuters*, September 12, 2013, http://www.reuters.com/article/2013/09/12/net-us-usa-security-snowden-brazil-idUSBRE98B14R20130912.

13 "Is Data Protection Agency Going To Censor The Internet?" *Reporters Without Borders*, February 26, 2013, http://en.rsf.org/spain-is-data-protection-agency-going-to-26-02-2013,44129.html.

14 Frances Robinson and Sam Schechner, "France Pushes EU to Regulate U.S. Internet Companies," *Wall Street Journal*, September 19, 2013, http://online.wsj.com/article/SB10001424127887324492604579085222987377040.html.

15 "Tobacco advertising," on the Australian Government Department of Health website, last modified June 19, 2013, http://www.health.gov.au/internet/main/publishing.nsf/Content/tobacco-advert.

16 Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired*, September 13, 2013, http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/.

17 European Parliament, "Act together to counter cyber attacks, urges Civil Liberties Committee," news release, June 6, 2013, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20130603IPR11005%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN.

18 Russian Federation, "Proposals for the Work of the Conference: Revision 1 to Document 27-E" (International Telecommunication Union, November 17, 2012), http://www.soumu.go.jp/main_content/000188224.pdf.

19 Declan McCullagh, "U.S. Seeks Veto Powers Over New Domain Names," *CBS News*, February 7, 2011, http://www.cbsnews.com/news/us-seeks-veto-powers-over-new-domain-names/.

20 Joshua Rosenberg, "India's Proposed 'Registration' Plan Is a Market Access Barrier," *ITI Policy Blog*, September 24, 2013, http://blog.itic.org/blog/indias-proposed-registration-plan-is-a-market-access-barrier. See also: Office of the U.S. Trade Representative, "2013 Section 1377 Review on Compliance with Telecommunications Trade Agreements" (USTR, April 2013), http://www.ustr.gov/sites/default/files/04032013%202013%20SECTION%201377%20Review.pdf.

21 Matthew Broersma, "IETF Slams ITU Standards Vote," *TechWeek Europe*, March 1, 2011, http://www.techweekeurope.co.uk/news/ietf-slams-itu-standards-vote-22392; Iljitsch van Beijnum,"ITU bellheads and IETF netheads clash over transport networks," *ArsTechnica*, March 3, 2011, http://arstechnica.com/tech-policy/2011/03/itu-bellheads-and-ietf-netheads-clash-over-mpls-tp/.

22 Christopher Painter, Daniel Sepulveda, and Uzra Zeya, "Internet Freedom for All," *DipNote* (blog), U.S. Department of State, August 13, 2013, http://blogs.state.gov/stories/2013/08/13/internet-freedom-all; "Say No To Online Censorship," on the Electronic Frontier Foundation website, accessed July 8, 2014, https://www.eff.org/pages/say-no-to-online-censorship.

23 John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation*, February 8, 1996, https://projects.eff.org/~barlow/Declaration-Final.html; Daniel Castro, "A Declaration of the Interdependence of Cyberspace," *ComputerWorld*, February 8, 2013, http://www.computerworld.com/s/article/9236603/A_Declaration_of_the_Interdependence_of_Cyberspace?pageNumber=1.

24 "Internet Freedom," *Foreign Policy*, January 21, 2010, http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom.

25 Kemina Kiss, "An online Magna Carta: Berners-Lee calls for bill of rights for web," *Guardian*, March 11, 2014, http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web.

26 "WikiLeaks: About," *WikiLeaks*, accessed July 8, 2014, http://wikileaks.org/wiki/WikiLeaks:About.

27 "Communiqué on Principles for Internet Policy-making" (OECD High Level Meeting: The Internet Economy: Generating Innovation and Growth, Paris, June 28-29, 2011), http://www.oecd.org/dataoecd/40/21/48289796.pdf.

28 "IDEA," on The Aspen Institute website, accessed July 8, 2014, http://www.aspeninstitute.org/policy-work/communications-society/programs-topic/global-projects/idea.

29 Global Agenda Council on Informed Societies, "Informed Societies: Towards a Code of Conduct for Government Leaders" (World Economic Forum, 2012), http://www3.weforum.org/docs/WEF_GAC_InformedSocieties_CodeConductGovernmentLeaders_Summary_2012.pdf.

30 "Frequently Asked Questions," on the Global Network Initiative website, accessed July 8, 2014, https://globalnetworkinitiative.org/faq/index.php.

31 Office of the U.S. Trade Representative, "European Union-United States Trade Principles for Information and Communication Technology Services" (USTR, April 4, 2011), http://www.ustr.gov/webfm_send/2780.

32 European Commission, "Commission proposes a comprehensive reform of the data protection rules" (European Commission, December 1, 2012), http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

33 National Telecommunications and Information Administration, "NTIA Announces Intent to Transition Key Internet Domain Name Functions," news release, March 14, 2014, http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

34 See: "Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography" (United Nations, May 25, 2000), http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx.

35 In contrast, within the United States, individual states should not impose their own e-commerce taxes because this imposes externalities on other states, and the Commerce Clause in the U.S. Constitution restrains states from placing burdens on interstate commerce. For more, see: Scott Andes and Rob Atkinson, "A Policymaker's Guide to Internet Tax" (ITIF, March 2013), http://www2.itif.org/2013-policymakers-guide-internet-tax.pdf.

36 Sawatree Suksri, Siriphon Kusonsinwut, and Orapin Yingyongpathana, "Impact of Computer-related Crime Act of 2007 and State Policies on the Right to Freedom of Expression" (Freedom of Expression Documentation Centre, iLaw, n.d.), http://www.th.boell.org/sites/default/files/computercrimeresearch.pdf.

37 Max Colchester, "Discounted E-Books Spark Outcry From French Shops," *Wall Street Journal*, September 24, 2010, http://online.wsj.com/article/SB10001424052748704814204575507910648793610.html. See also: "French law targets free shipping for Amazon books," *Deutsche Welle*, March 3, 2013, http://www.dw.de/french-law-targets-free-shipping-for-amazon-books/a-17133862, and Sam Schechner, "France Proposes Law Forbidding Book Discounts on Web," *Wall Street Journal*, October 3, 2013, http://online.wsj.com/article/SB10001424052702303492504579113513328860216.html?mod=djemITP_h&cb=logged0.9502857003826648.

38 "WTO: US Internet Gambling Ban Illegal, Orders Annual Trade Sanctions," *Yahoo!*, December 23, 2007, http://voices.yahoo.com/wto-us-internet-gambling-ban-illegal-orders-annual-741435.html.

39 There do not appear to be international conventions on online gambling. See: Marketa Trimble, "Proposal for an International Convention on Online Gambling" (University of Nevada, William S. Boyd School of Law, June 19, 2012), http://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1715&context=facpub.

40 "United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services" (World Trade Organization, March 13, 2013), http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm.

41 "China approves tighter rules on internet access," *BBC News*, December 28, 2012, http://www.bbc.co.uk/news/world-asia-20857480.

42 Ben Blanchard, Sally Huang, and Nick Macfie, "China tightens Internet controls, legalizes post deletion," *Reuters*, December 28, 2012, http://www.reuters.com/article/2012/12/28/net-us-china-internet-idUSBRE8BO01320121228.

43 Ashley Chia, "Amendment to Copyright Act aim to stop online piracy," *Singapore Law Watch*, July 9, 2014.

44 "TRIPS: Agreement on trade-related aspects of intellectual property rights, PART II—Standards concerning the availability, scope and use of Intellectual Property Rights" (World Trade Organization, n.d.), http://www.wto.org/english/tratop_e/trips_e/t_agm3_e.htm.

45 Loek Essers, "Google Video trial to continue to Italian supreme court," *PCWorld*, April 17, 2013, http://www.pcworld.com/article/2035387/google-video-trial-to-continue-to-italian-supreme-court.html.

46 "DNS Extension for Autonomous Internet (AIP)" (Internet Engineering Task Force, December 13, 2012), http://tools.ietf.org/html/draft-diao-aip-dns-00.

47 For a less technical summary, see: Kevin Murphy, "China proposes to split up the DNS," *DomainIncite.com*, June 18, 2012, http://domainincite.com/9474-china-proposes-to-split-up-the-dns.

48 In this case, the proposal appears to have received little support to move forward.

49 The European "Right to be Forgotten" is a good example of this.

ACKNOWLEDGEMENTS

The authors wish to thank the following individuals for providing input to this report: Bethany Imondi, Alex Key and Elizabeth Stewart. Any errors or omissions are the authors' alone.

ABOUT THE AUTHORS

Daniel Castro is a Senior Analyst with the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

Dr. Robert Atkinson is the President of the Information Technology and Innovation Foundation. He is also the author of the books *Innovation Economics: the Race for Global Advantage* (Yale, 2012) and *The Past and Future of America's Economy: Long Waves of Innovation that Power Cycles of Growth* (Edward Elgar, 2005). Dr. Atkinson received his Ph.D. in City and Regional Planning from the University of North Carolina at Chapel Hill in 1989.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION, CONTACT ITIF BY PHONE AT 202.449.1351, BY EMAIL AT MAIL@ITIF.ORG, ONLINE AT WWW.ITIF.ORG, JOIN ITIF ON LINKEDIN OR FOLLOW ITIF ON TWITTER @ITIFDC AND ON FACEBOOK.COM/INNOVATIONPOLICY