

A Third Way Framework for Global E-Commerce

Progressive Policy Institute
Technology & New Economy Project

Shane Ham and Robert D. Atkinson

March 2001

Contents

Introduction	3
Six Principles to Guide the Development of Global E-Commerce	4
Why Focus on B2C?	8
Jurisdiction: The Global E-Commerce Lynchpin	9
Two Views on Global E-Commerce Jurisdiction	9
Finding a Third Way	11
Applying the Framework	14
Taxation and Tariffs	14
Privacy	16
Consumer Protection.....	17
Regulation of Services	18
Content Restrictions	19
Rogue Actors	20
Policy Recommendations.....	22
Conclusion	23
Endnotes.....	25

Introduction

The Internet is dramatically expanding opportunities for business-to-business (B2B) and business-to-consumer (B2C) e-commerce transactions across borders. For B2C transactions especially, the Internet sets up a potential revolution in global commerce: the individualization of trade. It gives consumers the ability to conduct a transaction directly with a foreign seller without traveling to the seller's country. While this could be done in the past by post, telegram, phone, or fax, such sales were relatively rare because the consumer had to know in advance where to make contact and what to buy. The Internet allows sellers to put their storefronts, in the form of Web pages, in front of consumers all over the world. Technology has expanded the consumer marketplace to an unprecedented degree, and it will change the way we think about trade. The implications of this for economic development, globalization, and cultural exchange are immense. This creates opportunities for both consumers and small enterprises that must not be squandered.

But for all the potential of global e-commerce, there are countless vexing policy questions to be worked out, any one of which can threaten the viability of this nascent form of trade. **All of the Internet issues being debated in the United**

States—consumer protection, data privacy, taxation, content regulation, copyright, spam, technology deployment, and many more—need to be resolved at the international level as well. However, unlike the United States, which has a federal government and a constitutional guarantee of free trade, global e-commerce faces two additional serious complications: no central international authority to make the rules and regulations and no uniform commitment to global free trade. Moreover, conducting electronic commerce across national borders adds many more policy issues to the mix—jurisdiction, customs duties, import and export restrictions, intellectual property licensing, and more—that are only now being examined.

To promote the growth of global e-commerce, policymakers must find the Third Way on two basic conflicts: jurisdiction and sovereignty. Jurisdiction refers to the question of whose rules will apply to a transaction when the buyer and seller (or host and viewer) are located in different countries.¹ Applying the rules of the buyer's country would force sellers either to identify and comply with the differing and sometimes contradictory laws of every country or to forego sales to foreign buyers.

Applying the rules of the seller's country, on the other hand, with no other provisions or protections will force buyers to give up valuable consumer protections, making them less likely to buy from foreign Web sites. **The Progressive Policy Institute (PPI) believes that a Third Way must be crafted on the jurisdiction issue, constructing a system in which sellers are not subjected inadvertently to the laws of other countries while employing new technologies, improved information systems, and updated international rules that protect consumers and create an environment of trust.**

The second conflict is sovereignty, the question of how much domestic control over access to the global Internet must be relinquished in order to promote global e-commerce. A large amount of content (e.g., political, sexual, religious, gambling) residing in cyberspace, while legal in the country from which it originates, is considered illegal in many other countries. (This is especially true of content posted by users in the United States, where the First Amendment protects speech that would be illegal in many places around the world.) To allow one country to exercise control over content posted by citizens of another would allow that country to "reach out" into other sovereign nations and tamper with the rights of their citizens, thereby effectively giving control of cyberspace to the country with the most restrictive laws. At the same time, if governments have no ability to control their own citizens' access to illegal content, those governments could reduce or sever all connections to the Internet, which would drastically limit global e-commerce. **Here, too, PPI believes that a Third Way can be achieved with respect to sovereignty, one that does not let individual nations reach beyond their own borders to control content in cyberspace but does let them control both users and Internet hosts within their borders, as long as the content controlled is not governed by trade agreements.** This paper sets forth principles toward achieving Third Way solutions to these two basic questions and demonstrates how those principles might be applied to policy issues such as privacy, consumer protection, taxation, and content control.

Six Principles to Guide the Development of Global E-Commerce

1. Take a cautious approach to regulation: Allow global e-commerce time to develop before determining which areas will require government action.

There are two major threats to global e-commerce. One is rushing to impose legal and regulatory frameworks before gaining a full understanding of the issues and needs involved. Though it is easy to imagine any number of problems that governments might seek to solve, to do so at this early stage could be counterproductive. Cross border business-to-consumer transactions represent a brand new form of trade; the old ways of regulating trade will not work on the Internet. As noted below, innovative solutions ranging from international treaties to online dispute resolution mechanisms may be able to meet the goals of regulation—mitigating the risks to buyers and sellers without engaging the troubling jurisdiction questions of the old economy.

The other threat, however, is doing nothing. Global e-commerce faces many "natural" barriers, including language, currency, and cultural differences; overseas shipping costs; and national brand identification. If nothing is done, the natural tendency will be for e-commerce to become balkanized into local zones, with consumers visiting only sites in their own country or a small number of countries with which they feel comfortable.² In order to realize fully the benefits of global e-commerce, governments must lend a helping hand where necessary to reduce the risks of cross border transactions, but it will take time to determine when and where government action can be used effectively.

2. Increase global market access: Maximize opportunities for buyers and sellers to come together.

Empowering consumers and sellers—especially small enterprises—by expanding market access should be the main goal of any government action (or forbearance of action) regarding global e-commerce. The reasons for this are basic, but

very important. First, a larger market lowers the marginal costs associated with running Internet-based businesses, allowing the companies to spread their fixed costs over more customers, which lowers prices. E-commerce will become more efficient and less costly by gaining global economies of scale. Greater market access also gives small entrepreneurial ventures a better chance at success: a comic book store at a local strip mall selling to nearby residents may have a hard time, because comic book buyers are a niche market and the number of customers is small, whereas an online comic book store selling around the world stands a much better chance in a larger customer pool. Low cost access to global markets is especially important for ventures in developing nations, which can use the power of global e-commerce to “leapfrog” their economic development efforts and sell to an array of wealthier consumers.³

Second, a global Internet provides consumers with global choice. Shopping “bots”—automated buyer agents that seek out the best price on a given item—are increasing in popularity, and promise to bring tremendous efficiency to the pricing of goods and services on the Internet.⁴ Expanding the bot’s range, from national to international, will encourage competition and reduce prices. Moreover, the Internet is not just a retailing channel—diverse services and media can be delivered over ever-expanding broadband networks, creating new business opportunities for communications, information, and entertainment ventures. Greater market access gives all of these businesses, in whatever country they happen to be located, a better chance at success, and gives consumers of all nations a broader choice of goods and services.

Finally, as the infrastructure and systems to facilitate global e-commerce develop, access will also be increased in a more important market: the marketplace of ideas. History has taught us time and again that trade is the most powerful catalyst for cultural exchange and greater understanding between societies. By creating an environment for businesses to forge ahead with direct cross-border contacts with consumers, those same infrastructures will be used to bring together Internet users from around the world.⁵

3. Don’t use regulations for protectionism: Signatories to the World Trade Organization (WTO) or other multilateral trade agreements should not be allowed to impose rules on e-commerce or the Internet with the intent of reducing on-line foreign competition.

The practice of protecting domestic producers through the use of subtle or seemingly unrelated regulations is an old one, but the growth of global e-commerce presents the opportunity to take it to a new level. The complexities of the technology, the legal issues involved, and the innovative business relationships between companies that conduct and facilitate e-commerce all lend themselves to regulations protecting domestic industries not only from foreign competitors, but from electronic commerce itself.⁶ The pressure for such regulations is likely to be amplified by the burgeoning anti-globalization movement (exemplified by the 1999 WTO protests in Seattle and the presidential candidacy of Ralph Nader).

As global e-commerce grows, the WTO will see more disputes about regulations aimed at the Internet and designed to give advantage to domestic industries. Examples include requiring Web sites to be delivered in the country’s native language, requiring transactions to occur in the country’s currency, requiring certain licenses or certifications to operate or use electronic equipment within the country, or requiring the use of nonstandard security protocols. Even more troubling is the process by which some of these regulations likely will be derived: the stoking of nationalistic fears that a country is being left behind in the new world economy. The initial lead that the United States holds in e-commerce will create political controversies in other countries that are ripe for the use of nationalism as a tool to gain competitive advantage, or at least slow the incursion of foreign e-commerce to allow domestic industries to catch up: an electronic version of the McDonald’s controversy in France.⁷ Countries that use such tactics might gain in the short run, but over the long run they will limit their standard of living and hinder global e-commerce. Rather than try to create rules and regulations to limit global e-commerce, nations would be better off pursuing policies

designed to build a robust digital domestic economy (e.g. telecommunications reform, including flat-rate call pricing for Internet access; digital government; deregulation; and technology investment).

4. Enforce regulations domestically: Governments cannot impose their laws on foreign companies unless those companies target their activities within the government’s territory or a treaty is in effect.

In the off-line world, activities engaged in by citizens of one country don’t normally affect the citizens of another country unless those activities are specifically aimed at them (such as sending international mail). The online world should be no different. An online business based in one country cannot be expected to comply with the laws of other countries—such as privacy regulations or marketing restrictions—merely because their Web site is accessible in other countries.

On the other hand, if the Internet seller targets its goods or services to citizens of another country, that seller should be prepared to comply with the laws of that country. (For more detail on what activity might constitute targeting, see below.) Targeting must subject a seller to the targeted country’s jurisdiction in order to prevent companies from relocating offshore to avoid local laws, a situation that would encourage the rise of cyberhavens (discussed below). Put another way, a government cannot “reach out” and exercise authority in another country, but it can exercise authority if someone in another country “reaches in” to consumers in its jurisdiction. Similarly, if two nations are part of a bilateral or multilateral trade agreement that imposes requirements on Web sites, then Web sites in both nations must comply with the terms of that agreement.

5. Limit restrictions on social, cultural, and political content: Government restrictions on content cannot block trade

in violation of World Trade Organization principles and must be enforced only within the restricting government’s territory.

Given the wide variety of objectionable material available on the Internet, it is no surprise that some governments may seek to keep their citizens from accessing some content. Disputes in this vein are already arising for content that portrays or promotes racial hatred, violence, sexual activity, or drug use, to name a few. These issues go to the very heart of national sovereignty. In the United States, where the constitutional guarantee of free speech has become ingrained

A government cannot “reach out” and exercise authority in another country, but it can exercise authority if someone in another country “reaches in” to consumers in its jurisdiction.

in the culture, public sentiment is likely to come down on the side of more freedom, but the United States cannot impose that sentiment on other

sovereign nations. For instance, we do not like China’s restriction of access to certain online information, but we are powerless to stop it, just as the Chinese government is powerless to demand that the U.S. government block Chinese access to U.S. sites critical of China. Moreover, policies for global e-commerce should not be used as bargaining levers for these non-economic disputes over freedom and human rights; if Internet technology is made to bear responsibility for intractable social and political disagreements, it will not succeed.

But if governments choose to exercise control over the foreign Internet content that their citizens may access, every nation must demand that every other nation adhere to two conditions. The first is that such controls must apply only to cultural, social, and political content, not trade. Nations that are signatories to the WTO have agreed to a set of principles to facilitate international trade and to a process for resolving disputes.⁸ Though the Internet will change the character of a portion of international trade transactions, there is no need to scrap the hard-won international cooperation that the WTO represents. Claims of cultural or political infringement should not be used as a back door method of discrimination against imports. If a country restricts global e-commerce on grounds

that are (explicitly or implicitly) trade related rather than cultural or political, the WTO can and should take up the matter in the established dispute resolution process.⁹

The second condition is that all content controls must be implemented domestically. In keeping with Principle 4 above, governments cannot “reach out” to shut down Internet operators that reside outside of their jurisdiction. Governments must control content through laws and regulations that apply to their own citizens, such as requiring Internet Service Providers to filter certain content or punishing individual users for downloading prohibited content. (See section on Content Restrictions below.) Of course, exercising control over every citizen’s Internet behavior, while technically possible, requires control over the technology and communications infrastructure that only a few governments are likely to exercise.¹⁰ Inherent in the spread of Internet technology and the attendant economic benefits is a realization that the more time citizens spend in cyberspace, the less control their governments will have over them. This is why expansion of global e-commerce must be balanced with respect for sovereignty; if a government feels that the trade-off between commerce and social stability is not in its interest, the former is more likely to be rejected.

6. Take advantage of technology: Encourage innovation in the development of technological tools and industry best practices that solve public policy problems.

Not every problem needs to be addressed by government regulation, especially with regard to the Internet. The Internet lends itself to creative solutions to policy problems precisely because software is a powerful tool to give people the ability to manage their own transactions.

Many technological solutions are being developed to facilitate an efficient and trusted environment for both buyers and sellers. One of

the best examples is the Platform for Privacy Preferences Project (P3P).¹¹ The project of the World Wide Web Consortium (W3C)¹² is creating a system that allows browsers to look at a Web page’s underlying source code to determine the privacy policy that covers the page; if the privacy level is below a predetermined level set by the user, the Web browser (or other P3P implementation tool) will warn the user. This consumer-empowering technology, when fully implemented, may help alleviate the desire for strict government controls on data privacy practices and facilitate easier negotiation between nations with different privacy regimes.¹³ Technology promises other

solutions as well, in areas from language translation to content control to dispute resolution. Policymakers should turn to technology whenever possible

and, more importantly, they should think in terms of what technology could do in the future rather than what it can do now.

In order to facilitate the growth of global e-commerce, PPI makes the following proposals, discussed in more detail in the ***Policy Recommendations*** chapter of this paper:

- **stay within the current international trade framework;**
- **make the moratorium on tariffs for electronic transmissions permanent;**
- **treat digitally delivered products as intangible goods;**
- **eliminate tariffs on small-value transactions;**
- **work with third parties seeking to provide solutions;**
- **promote consumer education efforts; and**
- **draft and enact global treaties governing criminal activity on the Internet.**

Why Focus on B2C?

In the coming years, the majority of e-commerce, both domestic and international, will be business-to-business transactions. The Internet will bring tremendous benefits to B2B trade, by cutting costs and improving efficiencies. It will also allow for the development of new business relationships, new pricing strategies, and bring about a general decrease in “friction” in international markets. The explosive growth of global B2B marketplaces has created tremendous opportunities for entrepreneurial suppliers who might otherwise go unnoticed.¹⁴ While none of these advances should be minimized, the future of international B2B e-commerce will by and large remain an extension of the past: commerce conducted between either sophisticated international merchants who have advanced knowledge of the trade system or newcomers who must hire consultants to navigate the trade system and protect their interests against the sophisticated merchants. For these players, the Internet is basically a powerful new communications and transactions tool.

Business to consumer transactions, while representing a smaller volume of online trade, will provide special benefits to consumers. Creating a global marketplace will increase the benefits of competition, provide a broader range of products and services, and in the case of digital delivery, will virtually eliminate manufacturing

and transportation costs. Moreover, prices will be reduced by eliminating exporter and importer middlemen that exist to surmount the complexities of trade bureaucracies.

For the revolution to succeed, however, the complexities must either be removed from the process or made transparent. If cross-border B2C transactions are to work, a consumer needs to make an informed decision before a transaction is completed: what the product or service will be, how much it will cost (including taxes, duties, and shipping), how the company will use the consumer’s personal data, and what the rights and responsibilities of both parties will be if a dispute should arise.

As noted above, these cross-border transactions, with the buyer located in one jurisdiction and the seller in another, are a novel development and will require a new way of thinking about trade. Policymakers, therefore, will have to pay special attention to the problems of cross-border B2C transactions if this new type of commerce is to flourish. Effort expended now to resolve these problems will pay dividends for decades. On the other hand, rushing to impose strict regulatory structures over this uncharted territory could drastically restrict international B2C trade.¹⁵ Reaching consensus on new and unforeseen policy issues will almost certainly involve mistakes and lost time and money for both consumers and businesses. But if pursued properly, however, the rewards will be immense.

Jurisdiction: The Global E-Commerce Lynchpin

A central issue raised by the growth of the Internet is that of international jurisdiction. Traditionally, jurisdiction has been a matter of the sovereign power of a state over the territory within its physical borders. The Internet has thrown that notion into chaos. Now, a person located in Country A can engage in a transaction on behalf of a business established in Country B by connecting to a server located in Country C through an Internet Service Provider (ISP) headquartered in Country D, selling to a purchaser in Country E who wants the product delivered directly to a relative living in Country F. The legal and regulatory complications of such a transaction are far greater, obviously, than those encountered at the local shopping mall.

With so many jurisdictions involved, uncertainties arise as to the rules and mechanisms that will protect the interests of both businesses and consumers.¹⁶ Rather than face those uncertainties, both businesses and consumers are likely to stick to domestic B2C transactions. **Growth of global B2C electronic commerce, therefore, will require either a resolution of the unique jurisdictional issues involved (which we believe will happen in the distant future, if ever), or the establishment of some other regime that can promote an environment of trust for**

both parties to an international transaction and is effective enough to forestall jurisdictional disputes, perhaps indefinitely.

Two Views on Global E-Commerce Jurisdiction

As the debate over global e-commerce unfolds, the debate over jurisdiction has split into two basic camps: those who believe that a cross-border electronic transaction can be defined as taking place in only one country, and those who seek to eliminate problems of jurisdiction by making the laws and regulations the same in every country through harmonization.

For those who want a single country system, an obvious question arises: in which country did the transaction occur? In other words, did the seller come to the buyer's country (country of destination) or the buyer come to the seller's country (country of origin)? The country of destination view is held largely by government regulators and consumer rights advocates. This view arises from the basic assumption that consumers are at a disadvantage during a cross-border transaction, and therefore should be the presumptive beneficiary of the legal regime governing the transaction.

Intuitively this view seems correct. A consumer in the United States looking to purchase an item is accustomed to the assumption, backed by the truth in advertising laws of the U.S. government, that the item will work as advertised and that it can be exchanged or returned if it does not. If that consumer purchases the same item over the Internet from a company located in a foreign country, the consumer is likely to assume that the laws he is accustomed to will still protect him, that the product will do what the seller says it will do, and that it can be returned if it does not. The fact that the consumer makes decisions based on that assumption indicates the need for the laws of the consumer's country to apply. Put another way, why should a foreign company be able to falsely advertise to a U.S. citizen located in U.S. sovereign territory if a domestic company is forbidden to do so?

It is perfectly understandable that governments would seek to extend the protection of their citizens into cyberspace, but such a regime would raise the costs of global e-commerce and reduce the number of companies engaging in it. Learning and complying with a myriad of different and sometimes conflicting laws governing commerce can place a tremendous burden on companies, especially small businesses.¹⁷ It is unreasonable to require those companies to comply with the laws of nearly 200 countries around the world; moreover, such an undertaking would never be justified by the revenue returned. **The country of destination rule, therefore, is unworkable; attempts to resolve jurisdictional issues under this rule will only hinder the growth of global e-commerce.**

Following a strict country of origin¹⁸ rule, as many businesses favor, might seem to get around the compliance problem, as buyers are better positioned to assume the burden of factoring differing government regulations into the purchasing decision. Tourists traveling abroad, after all, frequently demonstrate their willingness to buy while subject to the laws of the country they are visiting. There is a major difference, however, between a tourist and an Internet shopper: The tourist can physically examine the item before purchase, and can guarantee delivery by taking an item with her. Buying a \$200 rug from a street peddler in Acapulco is a relatively

risk-free transaction; buying the same rug from the same peddler over the Internet is considerably more risky.

A reliable and easily accessible dispute resolution process, both for innocent misunderstandings and outright fraud, is a key part of the environment of trust necessary to online transactions, but the traditional providers of that process—the courts—are unavailable under a strict country of origin rule. Filing a lawsuit against a foreign seller in a foreign country is more hassle than an average consumer is able or willing to endure. For that reason, the consumer looking for that \$200 rug over the Internet will probably purchase it from a local retailer rather than directly from the seller in Acapulco, even if the imported rug is marked up to \$250, because the consumer has the assurances of his own laws and the ability bring the retailer to court and win an enforceable judgment if necessary. The local retailer would hold this advantage even if the Acapulco seller's Web site had featured full disclosure of the rules under which it was operating; the rules are meaningless if the expense of enforcing them is greater than the price of the item. **A regime in which the seller has no practically enforceable legal obligations in the buyer's country, as is the case in a country of origin regime, will not lead to the growth of global e-commerce.**

Advocates of harmonization, on the other hand, seek to simplify global e-commerce by eliminating differences in the regulatory and tax structures that govern such transactions. Harmonization has obvious benefits: It would provide a predictable environment for businesses and consumers alike, no matter which borders a particular transaction crosses. Moreover, unscrupulous businesses would have no incentive to establish headquarters in small nations with lax regulations and enforcement. (See the section on Rogue Actors below.) Indeed, harmonization would eliminate the need to ascertain the location of either the business or the consumer, except when physical delivery of a product is necessary.

There will be, of course, high levels of international cooperation on those issues that have high levels of international agreement, such as rules governing the sale of narcotics, child pornography, endangered species, and

military hardware. But full harmonization will not only be difficult to achieve, it is not something we should aspire to achieve. Flexibility, rather than monolithic global law, is a better model for the competitive environment of the New Economy. For example, the United States has not chosen to impose an “opt in” standard for online data privacy, but such a law might emerge if all nations had to agree on one privacy law, thereby reducing the flexibility of all U.S. Internet firms, even those that do not sell to foreign consumers. Moreover, full harmonization would also likely be viewed as a major step toward global government.¹⁹ While many nations are working out the kinks of supranational governance on a regional basis, worldwide governance is a step few are prepared to take—does any country really want to give up its ability to make laws for its own citizens? Harmonization, then, is in most cases neither likely nor desirable.

Flexibility, rather than monolithic global law, is a better model for the competitive environment of the New Economy.

Finding a Third Way

While there is no magic bullet to the jurisdiction quandary, global B2C e-commerce is still a very real possibility. The challenge for policymakers will be to find a Third Way on these questions by blending governmental and private solutions to create a regime that provides a trusting environment for transactions across all borders, but at the same time does not burden e-commerce businesses with excessive costs and a tangle of contradictory laws and regulations. Such a regime might include the following:

- ***Jurisdiction based on targeting.*** Simply put, a company would be subject to the laws of another country if it targets its marketing efforts at consumers in that country; in other words, if the seller “goes to” the buyer’s country. The logic behind such a standard is unimpeachable—there are no grounds for jurisdiction if the business does not actively seek to be in that jurisdiction—but the technology of the Internet makes the

definition of targeting extremely complicated. A Web site may be marketed and promoted only in the seller’s own country, but it can be accessed anywhere in the world. Determining which sites target a country and which are merely accessible in that country is a key challenge.

Countries must agree, therefore, on what constitutes targeting; putting up a Web site in the United States written in Spanish would not necessarily target consumers in Spain, but advertising the Web site on a Madrid billboard would. Targeting might also occur if

the business placed ads on Spain-specific Web sites like Yahoo! Espana, or if the business offered special discounts to consumers in Spain. Physical presence in a country might also constitute targeting, but physical presence should not necessarily be taken as firm evidence of it; such a rule could discriminate against multinational corporations with foreign business units that are unrelated to their B2C enterprises. If a U.S. company Web site sells music CDs and also has a division located in France that makes and sells electronic goods, the Web site should not be subject to French laws unless the site explicitly markets to French citizens.

Any international agreement on targeting, however, must explicitly state that simply selling to a consumer in a country does not constitute targeting.²⁰ To do otherwise would create a default “country of destination” rule—sellers would be forced to refuse customers from other countries in order to maintain their freedom from jurisdiction in those countries. Consumers should be able to buy from any site on the Internet (subject to the laws of their country), but that can only happen if sellers feel free to transact with consumers that were not targeted but nevertheless came to the site voluntarily and asked to make a purchase.

This rule is especially important to operators of political and human rights Web sites. If a Web site run by exiled dissidents

protesting a repressive government could be said to be targeting citizens in that repressive nation, political dissent on the Internet could be severely curtailed. On the other hand, nations that sign a targeting treaty must have recourse against objectionable material that is aggressively targeted to their citizens, as a neo-Nazi hate site might be aggressively targeted at Germany by “spamming” German e-mail accounts or posting the URL on German electronic bulletin boards. **A targeting treaty must make clear that content that merely exists in cyberspace (and is not promoted through direct e-mail or other methods) cannot be considered targeting a foreign country, even if unsolicited interaction occurs with users in that country.**

- **Safe Harbor Agreements.** Governments with different regulatory approaches to e-commerce issues can ease the way for global e-commerce with safe harbor agreements. These agreements can be negotiated between two countries to “bridge the gap” when the laws and regulations of the two countries are too different for mutual recognition. Under a safe harbor agreement, a set of rules or principles is negotiated that are less strict than the regulations of the more stringent country but more strict than those in the less stringent country. Businesses in the less stringent country must meet the conditions of the safe harbor agreement if and only if they wish to conduct transactions with citizens of the more stringent country. Neither country needs to change its rules for domestic companies, and compliance is on a voluntary basis; a business can simply opt out of international sales to avoid the safe harbor rules. (An example is the recently ratified safe harbor agreement on data privacy negotiated by the United States and the European Union, discussed below.)

Safe harbor agreements can achieve some of the benefits of harmonization while maintaining respect for sovereignty. By creating a middle ground between different legal codes—with voluntary rather than mandatory compliance—governments can continue to regulate their businesses at the

level they feel is appropriate, and sellers will enjoy greater predictability and lower compliance costs, making global e-commerce more feasible both economically and politically.

- **Voluntary Transaction Contracts.** When a consumer wants to buy from a foreign Web site, and that Web site is not targeting the consumer’s country, the buyer and seller should be able to agree to the terms of the transaction privately and to enforce the contract privately. The buyer and seller can use the contract to decide choice of law—which country’s laws will apply to the transaction—and how disputes will be settled.

It is conceivable that transaction-based private contracts will constitute a de facto country of origin rule because the seller will choose the laws of his own country; after all, if the seller was prepared to obey the laws of the buyer’s country he would probably be targeting that country already. The power of private contracts, though, is that the buyer and seller can choose any law. A buyer in Sweden, for example, might want to make a purchase from a Web site based in Brazil. The Brazilian does not ordinarily do business with Swedish buyers, but does target his products to the United States (and therefore complies with all of the laws in the United States.). Rather than choose between Swedish law and Brazilian law, neither party having any familiarity with the other, both parties could agree to let U.S. law govern the contract.

Online alternative dispute resolution organizations can take the place of courts to make these private contracts work (see below). Buyers and sellers can agree to submit their disputes to binding arbitration conducted by third parties. Such a system would sidestep certain issues of jurisdiction while promoting the environment of trust necessary for the success of global e-commerce.

- **Codes and Seals.** In the absence of an international regulatory authority, robust self-regulation is critical to the future of global e-commerce. Industry codes of conduct and seal programs, which have been

growing on the domestic level, can be scaled to an international level. This could, for example, take the form of a global version of BBBOnline, the Better Business Bureau's code and seal program, which certifies that the business bearing the seal complies with a code of conduct set forth at the BBB Web site. Digital seals could also be informational in nature, with Web sites posting flags of each nation with which the Web site is in compliance (providing "notice"). Through proper consumer education, the seals could become shorthand for complicated sets of policies, and provide a level of comfort for buyers without the need for careful analysis of the Web site's complicated legal disclaimers.

- **Software.** Web browsers and other software can be developed to record a user's individual

preferences and transparently check Web sites for compliance with those preferences. P3P software, for example, can automatically determine whether a Web site with a machine readable privacy policy meets the standards of the user. Such a system could also be developed to determine the applicable consumer protection policies, for example, without requiring additional effort on the part of the user.

Through some combination of these and other programs, plus a reliance on Internet technology itself, an environment of trust can be formed and a workable system for global e-commerce can be built. It is impossible, however, to predict exactly what that system will look like. It is vitally important that policymakers allow for experimentation to determine the best way to build such a regime.

Applying the Framework

Given the newness of global e-commerce, it is difficult to envision how the system will work in the long run; indeed, it is difficult to anticipate all of the problems that will arise. It is useful nonetheless to consider how a Third Way policy framework, consistent with the principles set forth above, can be applied to some of the important issues of global e-commerce.

Taxation and Tariffs

The debate in the United States over the imposition of sales and use taxes on e-commerce transactions—a debate that has yet to be resolved—demonstrates the difficulty of reaching a consensus on the taxation issue. The multitude of state and local taxing jurisdictions, each with their own product classifications and tax rates, make the collection of such taxes a potential burden for Internet retailers. Global e-commerce will increase that burden tremendously. Nevertheless, as the number of cross-border e-commerce transactions grows, the pressure to resolve the associated issues of jurisdiction will grow not only in response to the public policy issues at stake, but also because of the desire to capture tax revenues associated with those transactions.

European countries, in particular, rely heavily on value-added taxes (VATs), a complicated version of the sales tax. Currently, taxes on cross-border transactions are levied on physical products during customs inspection (assuming that the seller has properly labeled the package, which many small Internet businesses do not), but taxes on digitally delivered products are collected only if the buyer reports the transaction. (For many U.S. e-commerce transactions that cross state borders, buyers are legally required to report and pay a use tax. Needless to say, compliance is low.) In order to prevent the problem of non-reporting by buyers, the European Commission has suggested that non-European Union businesses wishing to engage in e-commerce with EU member nations may be required to register in the European Union to collect and remit VATs.²¹ This is exactly the proposal that upsets businesses that conduct interstate e-commerce in the United States: shifting the burden of tax compliance from the buyer (who must deal with only one jurisdiction) to the seller (who must deal with multiple jurisdictions). Though the EU member nations have every right to collect taxes, requiring businesses outside of their jurisdiction to do so is problematic.²² Similarly, sellers outside the United States do not relish the thought of collecting and remitting sales taxes to each of the 50 states.

Tariffs—the customs duties imposed on imports to raise the cost relative to the same items produced domestically—also stand as barriers to cross-border B2C transactions (and, to a lesser extent, all forms of trade). Most obviously, the duties themselves increase the cost to the consumer. Tariffs on e-commerce may also spawn novel forms of protectionism, increasing the burden on the WTO to sort out unprecedented and technologically complicated disputes. Because there is no clear consensus, for instance, on the treatment of electronic transmissions (such as e-mail), the WTO members agreed in 1997 to a temporary moratorium on duties for such electronic transmissions. The United States (and PPI) favors making this moratorium permanent, but EU officials do not agree; the issue will be troubling in the coming years.

Adding to the complication is the dispute over the treatment of digitally delivered products, such as downloadable software and music. Some countries want to treat downloaded products as services rather than goods, largely because trade in services is governed by the General Agreement on Trade in Services (GATS), which permits more restrictive trade policies than is allowed for goods under the General Agreement on Tariffs and Trade (GATT).²³ Thus, a music CD shipped by Federal Express would be a good, but the same music downloaded in MP3 format would be a service.²⁴ Doing this, however, is not only logically inconsistent, but it could put such digital products at a competitive disadvantage to their physically delivered counterparts, thereby losing much of the economic benefit of digital technology. This dispute is heating up between the United States and the European Union.

The most significant tariff-related barrier, however, is customs procedure. Dealing with customs can be one of the most complicated parts of completing an international transaction, which is why many businesses either abdicate responsibility for the process or simply refuse to sell internationally. When a buyer in Austria, for example, purchases a music CD from a U.S. Web retailer, frequently the terms of the

agreement clearly state that the buyer is the “importer of record” and is responsible for all customs duties and taxes. The U.S. company would not make any attempt to determine what those duties and taxes might be, so the buyer must contact the customs office in order to determine the accurate final cost. The difficulty of negotiating this bureaucratic maze, as much as the expense, constitutes a significant hurdle to buyers seeking to purchase products from overseas.

Tariffs on e-commerce may also spawn novel forms of protectionism, increasing the burden on the WTO to sort out unprecedented and technologically complicated disputes.

In *Internet Taxation: A Software Solution*,²⁵ PPI addressed the issue of sales taxes on e-commerce within the United States. PPI advocates fair

and neutral treatment of e-commerce; consumers should not be able to avoid taxes simply by purchasing online (or by any remote sales method), nor should they have to pay extra taxes simply because they purchase online. We proposed that a centralized database of taxable items and rates be created, which would allow businesses to automatically run their transactions against the database and compute the proper tax. Though the cross-border nature of global e-commerce complicates the issue, a software solution may well be possible for taxes and tariffs on international transactions; though tax simplification and elimination of tariffs for certain B2C imports will help make a database solution easier, technology can do the heavy lifting to resolve the problem without forcing governments to overhaul their revenue collection systems.

Indeed, companies such as MyCustoms.com²⁶ are already sprouting on the Internet to provide such services. Sellers can sign up with MyCustoms and have their entire catalogs classified in the database for international customs. When a consumer in Austria buys a CD from a U.S. Web site, the MyCustoms database can be queried instantly for a compliance check (ensuring it is legal to sell the product to a customer in Austria) and to obtain information on the customs duties and taxes. This enables the Web site to report the complete price, including duties and taxes, to the buyer. When the transaction is completed, MyCustoms would

automatically generate all of the appropriate information, file the forms, and pay the duties and taxes directly to the Austrian government. The company would then reimburse MyCustoms for the duties and taxes paid, plus a service charge (a small percentage of the total transaction).

Some trade experts are skeptical about the concept. They believe that tariffs are so complicated and change so rapidly that no single database can hold all of the information. Duties on shirts, for instance, can vary depending on where the cloth was manufactured. Export and import restrictions can also be tricky. Singapore bans the importation of chewing gum;²⁷ it would be easy for the computer to block the shipment of a pack of Juicy Fruit to a Singapore address, but less obvious to block the shipment of a pack of baseball cards that contains chewing gum.

These problems are troubling, but not insurmountable. A database solution that gives sellers a single point of remittance for worldwide tariff and tax compliance is feasible, but it will require a commitment on the part of government agencies around the world to make their data easily available in a timely manner and to simplify their tax rates and systems to the greatest extent possible.²⁸ If a government chooses not to make its tax collection requirements conform to a database solution, however, that government should continue to rely on consumer-side compliance (use taxes or VAT reverse charges) rather than require foreign sellers to collect and remit taxes for them.²⁹

Privacy

Few issues are of greater concern to Internet users than privacy. Internet technology allows for the collection of personal information and online behavior data in ways that are scarcely imaginable to those without degrees in computer engineering. The data collected by Internet users is sometimes used in unsavory ways, such as sending unsolicited commercial e-mail (“spam”), and has the potential for significantly harmful uses, such as employment discrimination.

Different countries approach privacy in dramatically different ways. Some nations, including the United States, take a sectoral approach, mandating protections for sensitive

privacy areas (such as medical and financial data) while encouraging Internet companies to “self-regulate” by developing best practice standards and voluntary seal programs and placing the responsibility on the Internet users to vote with their clicks. Other countries, the EU countries in particular, feel that government regulation of privacy in the Internet space is necessary to protect their citizens. In 1998, the European Union adopted the Directive on Data Protection³⁰ which mandated strict privacy policies for any Web site that collects data from citizens of EU member states. Recognizing that the restrictions would effectively cut off global e-commerce for many U.S. companies, the U.S. government negotiated a safe harbor agreement with the European Union, which took effect in November 2000.³¹

The safe harbor agreement lists seven data privacy principles that U.S. companies must adhere to in order to be considered “adequate” under the Directive on Data Protection. Companies that wish to conduct business with citizens or firms in EU member states must certify to the U.S. government their compliance with the safe harbor principles, either by developing a privacy policy that meets the principles or by joining a third-party seal program that guarantees compliance with the principles. Joining the safe harbor is voluntary; those companies who do not receive personal data from individuals or organizations within the EU member states need not adhere to the safe harbor principles. Those businesses that choose to join the safe harbor benefit as well: The safe harbor principles are less restrictive than the Directive, and therefore compliance costs are lower.

The privacy safe harbor agreement is a model of intergovernmental cooperation to promote the growth of global e-commerce while respecting the sovereignty of the nations involved. It secures the benefits of harmonization (a predictable international regulatory environment) without impeding the ability of the governments on either side of the Atlantic to legislate domestic data privacy regulations. If this agreement proves workable in the long run, other safe harbor agreements may be struck on similarly troubling regulatory issues, such as marketing and advertising, unsolicited commercial e-mail, product safety, and so on.

Of course, the safe harbor agreement need not be the last word on international data privacy protections. Technological solutions such as P3P (discussed above) will, when fully implemented, empower Internet users around the world to make automatic privacy decisions with their Web browser software. This individual control may contribute more to the environment of trust than the safe harbor agreement, and points to the need to pursue a mix of solutions to the problems facing global e-commerce.

Consumer Protection

One of the biggest obstacles to global B2C e-commerce is lack of trust. Buyers will not go through the additional hassle of purchasing from a foreign company if they do not believe they will be protected in the case of a dispute or outright fraud. Because the court system is effectively unavailable for international transactions—due to cost and jurisdictional issues—buyers need an effective yet inexpensive dispute resolution system and a reasonable expectation that sellers will be accountable to that system. This can be provided by combining online alternative dispute resolution (ADR) with a seal program, as companies such as SquareTrade and others have done.

SquareTrade³² provides a low-fee, Internet-based mechanism for resolving disputes between buyers and sellers online by recognizing and taking advantage of a simple fact: In most cases, the parties to a dispute are capable of reaching a resolution, but anger and mistrust between them blocks their ability to negotiate that resolution. When a dispute is filed with SquareTrade, the parties can tell their side of the story in a free-form text box, but they are also required to answer a multiple-choice questionnaire. Based on the input of both parties, a computer automatically generates a list of options for resolving the dispute based on historical data from similar arbitrations. If the parties can agree on one of the computer-generated resolutions, the dispute is settled; if not, the dispute is transferred to a human mediator for further negotiation. If a resolution still cannot be reached, the dispute goes to binding arbitration.

There are several key advantages to a system like SquareTrade. First, the cost is low enough

to be feasible for the low-value transactions that are typical of B2C e-commerce. By automating the first level of negotiation, the expense of having highly trained arbitrators spend time on uncomplicated disputes is eliminated. Online ADR is also more fair than the current dispute resolution system of credit card chargebacks. While the chargeback capability creates trust for the buyer, who knows he can always get his money back if necessary, the seller is left vulnerable, because the chargebacks are usually done simply on the cardholder's word, absent some extraordinary proof on the seller's part. An unscrupulous buyer can take delivery and charge back the payment, effectively stealing the item.³³

The most important advantage of online ADR, however, is accessibility. Anyone can avail themselves of online ADR at any time, without having to take the time to go to court. Buyers and sellers in different countries can use online ADR to get around troubling questions of jurisdiction; there is no need to decide where a suit will be brought or under what law the suit will be decided. Knowing that an inexpensive and simple dispute resolution mechanism is available before a transaction is completed will make buyers more likely to buy at foreign Web sites, and knowing that the transaction will not subject the seller to a foreign jurisdiction will make sellers less likely to refuse transactions with foreign customers.³⁴

Of course, the effectiveness of online ADR depends on the willingness of both parties to abide by the final resolution. At the end of the process, both parties have a binding agreement, but if either party bails out, the other one still faces all of the tricky jurisdictional questions and the expense of enforcing a judgment in a distant country. This is where seal programs come into play. SquareTrade awards seals to sellers who agree to submit to the dispute resolution process and abide by the final resolution. If the seller fails to do either, the seal is revoked. A buyer that sees the seal, therefore, can be assured that the seller will deal in good faith (at least to the extent that SquareTrade can maintain the reputation of its seal program, which creates incentive for vigorous enforcement).³⁵

Online alternative dispute resolution will work only if businesses and consumers know of

its availability and trust in its capability to be inexpensive, impartial, transparent, and timely. Public education and the establishment of a strong track record will enable sites like Square-Trade to create the environment of trust to make international transactions feasible. In the long run, promotion of online ADR may prove to be a better investment of effort than dealing with some of the complicated jurisdictional issues related to global

e-commerce;

by effectively disposing of the vast majority of disputed cross-border transactions, ADR can turn

the few remaining disputes into legal curiosities rather than major public policy issues.³⁶

Other technology solutions can also be brought to bear to facilitate an environment of trust on a global basis. Databases of consumer protection laws—similar to tax/tariff databases—can be developed to inform consumers of the differences in legal protections between their country and the seller's. Seal programs similar to the Underwriters Laboratories (UL) and Good Housekeeping Seal of Approval can be developed to vouch for the safety and quality of products. Seal programs from different countries or regions could partner for mutual endorsements to give consumers the additional assurance of local evaluation of distant merchants or products. Given the myriad possibilities of technology for informing consumers and providing an environment of trust, non-governmental consumer protection for cross-border transactions may effectively facilitate global e-commerce.

Regulation of Services

The Internet has created tremendous new opportunities for all manner of cross-border service transactions, from banking to telemedicine. Traditionally, services have played a smaller part in the international trade system than goods, partly because many services require the seller and the buyer to be in close proximity—a problem that the Internet can eliminate.

A more important reason why cross-border services are limited, however, is the fact that the provision of many services is often heavily regulated by governments. The regulations are often designed to serve important public policy objectives. For example, regulations in telecommunications and delivery services were historically aimed at monopoly providers with universal service obligations; regulation in

financial services are aimed at economic stability. Regulations in the practice of medicine protect public health and

safety; regulations governing the practice of law are aimed at protecting consumers; regulations governing the advertising of securities trading are aimed at minimizing risk to individual investors. Technology is starting to break down these rationales, however, and because increased global competition in the provision of services will benefit all consumers, lowering barriers to competition is an important goal.

Because of the unique nature of services regulations, negotiations for liberalization occur under an agreement separate than the one for trade in goods. The General Agreement on Trade in Services, negotiated during the Uruguay Round, is different from the General Agreement on Tariffs and Trade in two important ways: National treatment obligations under GATS are on a sectoral, rather than general, basis and governments are given broad discretion to maintain limits on market access to foreign firms. Once a country commits to opening a service sector to foreign competition, however, GATS imposes obligations designed to maintain a level playing field, such as requiring all regulations to be transparent and applied evenly, and requiring governments to give foreign competitors equal access to the regulatory process.³⁷ However, GATS was negotiated and operates under the assumption that countries must be allowed to regulate the provision of certain services.³⁸

Though the growth of e-commerce has increased the pressure for liberalization of trade in

Given the myriad possibilities of technology for informing consumers and providing an environment of trust, non-governmental consumer protection for cross-border transactions may effectively facilitate global e-commerce.

services, the new environment has not fundamentally altered the basic principle that governments should be allowed to regulate services to whatever degree they wish, as long as foreign providers are treated fairly. This is especially true of services that require professional licensing, such as medicine or architecture; requiring foreign providers to meet the professional standards that domestic providers are required to meet is not discriminatory.

On the other hand, the temptation will exist to use regulations of service industries for

protectionist purposes, especially for long-entrenched monopolies that would not fare well against competition in the global market.

It is important, therefore, that policymakers recognize that the potential of the Internet, coupled with the accelerating trend toward deregulation of service industries and privatization of government service monopolies, provides a significant opportunity for increasing trade in global services. Increasing access to service markets across borders—particularly in sectors related to e-commerce such as telecommunications, marketing, business services, data processing, and so on—can be even more beneficial than increasing market access for goods. Governments should side with expanding cross-border service trade when considering current and future negotiation rounds of GATS. In addition, **regulations that discriminate against the cross-border delivery of services over the Internet (such as requiring a service provider to maintain an office within a country's borders, or onerous licensing requirements) should be subject to strict WTO scrutiny.**

Content Restrictions

The United States has attempted relatively little regulation of content on the Internet. This is not the case in many other countries. There are obvious examples such as China, which does not allow its citizens to view the Web sites of news organizations that have not been approved by the

government, but valid concerns over political, sexual, religious, or cultural content are likely to be reflected in regulations governing the Internet in many nations. In some European countries, for instance, it is illegal to sell Nazi memorabilia, or even to sell books that deny the reality of the Holocaust. (A French court ordered the U.S.-based Yahoo! auction site to block access to Nazi items that users have posted for sale; under pressure from

the ruling and from advocacy groups, Yahoo! voluntarily agreed to ban hate-related items from its auction site.)

The potential of the Internet, coupled with the accelerating trend toward deregulation of service industries and privatization of government service monopolies, provides a significant opportunity for increasing trade in global services.

Some countries do not allow marketing aimed directly at children, which will be a problem for many U.S. companies that blur the line between children's entertainment and advertising.³⁹ As more people from the Middle East and other countries with strong religious traditions become connected to the Internet, Web sites such as *Maxim* magazine or the *Sports Illustrated* swimsuit issue may be considered pornography by Web surfers in these nations. These issues are not merely economic; they involve deeply held values and beliefs, by nations who object to treating values as commodities or bargaining chips to be negotiated away in trade agreements.

In the past, physical geography has minimized clashes between differing laws and customs, but the increasing number of people on the Internet worldwide is changing that. The challenge for policymakers is to balance respect for sovereignty with increased market access. This poses two questions: To what extent should a government be allowed to control the Internet activity of its citizens, and by what mechanism can they exert that control?

The danger in allowing nations to ban domestically any form of global e-commerce they wish on social or political grounds is the temptation to use it as a justification for protectionism. **Consistent treatment must be the key to legitimate restrictions on international Internet access and commerce.** A government should only be allowed to ban its citizens from engaging in a cross-border

transaction if such a transaction would be banned if performed domestically, and if such a ban is consistent with the negotiated WTO framework—that is, if the treatment is nondiscriminatory. Inconsistent treatment of domestic and international transactions indicates insincerity in the claims of cultural infringement. This principle is fair on its face: A country can ban its citizens from viewing pornography on the Internet, for instance, but not if the citizens of that country can get unrestricted access to similar pornography at a local store. If a product or service is legitimate for domestic sales, it must be allowed for international e-commerce. Disagreements over what constitutes fairly blocked content and unfairly blocked commerce should be settled through the dispute resolution process at the WTO.

While there could be widespread international agreement to ban a few extremely objectionable types of content, such as child pornography, conflict between nations on content issues could be significant. **But, if a government wants to control what its citizens see or do in cyberspace, the burden of preventing access to cyberspace must fall on the government that seeks to block access, and that government can only impose such regulations on those entities over which it has prescriptive jurisdiction—Web site operators within its borders, its own citizens who surf the Internet, and foreign operators that target its citizens.**⁴⁰ Regulations could be imposed on domestic Internet Service Providers requiring that filters be put into place that block downstream access to forbidden sites. Technological solutions are currently in development that will allow the operators of Web sites to determine the precise physical location of a visitor, granting or blocking access accordingly.⁴¹ Laws could be passed regulating online behavior, punishing citizens when evidence of access to forbidden sites arises. (This is what the U.S. government does to citizens that download child pornography.)

None of these solutions will be 100 percent effective, and embracing any of them seems counterintuitive, as they all cut against the principle of increasing market access. The alternative, however, is much worse: Governments that view the Internet as a source of dangerous political subversion and cultural pollution, lacking an effective means to control

access to objectionable material, will prevent their citizens from becoming wired altogether. Respect for cultural and political laws around the world, even when it seems harmful in the short run, will promote the growth of the Internet and global e-commerce in the long run.

Rogue Actors

The most carefully constructed global e-commerce regime will still be vulnerable to those who refuse to play by the rules. The Internet, in fact, increases that vulnerability: an expanded market is just as beneficial to scam artists as it is to legitimate sellers, and the technology offers additional protection from capture and punishment. Taken as a part of the total number of cross-border transactions, unscrupulous actors are likely to be a tiny minority, but their impact—destruction of the environment of trust—may be disproportionately large.

The problem of fraud is nothing new, but the Internet does create new problems in dealing with it. Because buyers are not able to touch and examine up close the item they are buying, it is easier for sellers to get away with fraudulent representations of their products. It is also easier to disappear without a trace and reappear under a new name to avoid detection. There are unique ways to protect against fraud in global e-commerce, as outlined in the Consumer Protection section, but a certain number of scam artists will operate in cyberspace and use jurisdiction issues to help escape punishment.

A bigger worry, however, might be in what is legal. Some countries will undoubtedly tout themselves as cyberhavens, where lax regulations allow for Web-based businesses that would be illegal in most other countries. This has already happened with many online gambling sites, which are generally based in developing nations but accept wagers from anywhere. Cyberhavens could also spring up in less-traditional places like the Principality of Sealand, an abandoned WWII anti-aircraft platform six miles off the eastern coast of the United Kingdom that was occupied by former British army major Roy Bates and declared an independent country in 1967. (Since the British government failed to occupy or maintain the platform, they could no longer claim it as territory under the principle of international law known

as “dereliction of sovereignty.”) Sealand plans to host HavenCo, a data storage company that will offer users (potentially including criminals) complete anonymity, data security, and a sparse smattering of regulation.⁴²

Cyberhavens currently appeal only to businesses that are illegal in most countries, mainly because questions of jurisdiction are still unsettled. If court decisions bear out the viability of cyberhavens, however, it is likely that some Internet users—both buyers and sellers—will increasingly operate through servers located in the havens to avoid restrictions on their online behavior and legitimate government monitoring of their data traffic.⁴³ Given that ISPs in these cyberhavens remain intentionally ignorant of their customers’ activity—by providing complete anonymity and unbreakable data encryption—cyberhavens could present significant barriers to effective international law enforcement.

The services provided by companies in cyberhavens would not necessarily thrive on overwhelming demand by Internet users, as the online casinos do. Instead, for example, unsolicited commercial e-mail, or spam, could be launched from an anonymous server and sent to accounts all over the world. Laws on sending spam vary widely from country to country, but delivery of spam to an Internet user in a given country constitutes targeting in that country, which should obligate the sender to comply with the laws and regulations of the receiving country. To avoid compliance costs, unscrupulous spammers may resort to cyberhavens and, in doing so, create public outrage in many countries that would in turn translate to pressure for increased regulation of cross-border Internet traffic.⁴⁴

If sovereignty is to be respected, the problem of cyberhavens is a troubling one; a legal regime that would effectively eliminate cyberhavens would be so rigid as to severely restrict cross-border data flows and global e-commerce. **But because those cyberhaven countries are not likely to be members of the WTO, the global community will have to find innovative ways to put pressure on them to comply with international standards of conduct in cyberspace.** Legal and regulatory restrictions on the behavior of consumers and related businesses may also prove useful, such as the proposal to prohibit the use of credit cards and electronic funds transfers to online casinos as a way to

prevent Internet gambling.⁴⁵ Public education will also play an important role, empowering consumers to identify companies operating from cyberhavens and appropriately evaluate the risks.

Similarly, the growth of global e-commerce may decrease the effectiveness of economic sanctions. Businesses that are not allowed to export to a particular country due to sanctions may find the Internet to be an effective outlet for sales, particularly if the sanctions are imposed by a small number of countries. The classic example is the sale of Cuban cigars, a highly sought-after product that cannot be brought into the United States because of long-standing sanctions against the regime of Fidel Castro.⁴⁶ Cigar stores in the United States cannot sell Cuban cigars, but many cigar stores in Canada, Spain, the United Kingdom, and elsewhere have Web sites where the cigars can be purchased and shipped to the United States⁴⁷ Though global B2C e-commerce will not have a major economic impact on sanctioned nations—Iraq will not be able to sell crude oil over the Internet—the ability to easily find and buy products from sanctioned nations will tend to erode respect for the sanctions and, as a result, could erode the political will to use sanctions as a foreign policy tool.

Despite these issues, the existence of cyberhavens should not keep WTO member nations from developing appropriate laws and regulations for the Internet. On the one hand, cyberlibertarians argue that the presence of cyberhavens renders all laws over the Internet unenforceable and therefore moot. This argument ignores the ways in which pressure can be brought on nations that serve as cyberhavens, but more importantly, it ignores the importance of restricting undesirable behaviors domestically. On the other hand, some liberals argue that cyberhavens simply encourage a “race to the bottom” as companies relocate to countries with lax regulation. The vast majority of Internet companies, however, are legitimate business that have no desire to move to cyberhavens and lump themselves with shady and fraudulent ventures, especially if regulations in WTO countries are sufficient to provide a predictable environment without overburdening businesses. Governments with robust legal systems to govern the Internet can facilitate the growth of global e-commerce, while keeping the problems associated with cyberhavens to a minimum.

Policy Recommendations

There are a number of things decision makers around the world should do now to promote global e-commerce, but there are other areas where it is best to wait. Premature action may be counterproductive in the long run; a highly fragmented and burdensome legal and regulatory environment will complicate and reduce cross-border e-commerce transactions. Moreover, applying a burdensome regulatory framework to the Internet infrastructure, as some European nations want to do, will slow the growth of the Internet around the world. In the near term, protectionist policies also represent a significant threat to the growth of global e-commerce. It is important that policymakers do not negate their work in promoting cross border B2C transactions by condoning laws that destroy the ability of buyers and sellers to connect in cyberspace. Careful consultation with the stakeholders around the world will help prevent ill-advised policy decisions. As a result, policy makers should:

1. Stay within current international trade framework.

The Internet provides unprecedented opportunities for international B2C transactions, but the basic rules of international trade remain unchanged—there is no need for a radical

reconceptualization. **Member nations should adhere to the WTO principles for e-commerce just as they do for traditional importing and exporting.** Governments should also refrain from negotiating bilateral or multilateral e-commerce agreements that fall outside of the WTO principles.⁴⁸

Similarly, **there is no need for new institutions to treat global e-commerce as separate from the larger trade system.** Most governments have created international e-commerce working groups within established trade departments and ministries. Many non-governmental trade organizations—e.g. the Global Business Dialogue on Electronic Commerce (GBDe),⁴⁹ the Trans-Atlantic Business Dialogue (TABD)⁵⁰—also have programs for international e-commerce. Intergovernmental organizations such as the WTO,⁵¹ the Organization for Economic Cooperation and Development (OECD),⁵² and the Hague Conference on Private International Law⁵³ are also considering how e-commerce can fit into developed and developing international trade agreements.

Given the technical complexity of the Internet, it may be necessary to establish within the WTO a special panel of experts with the specific task of mediating e-commerce related disputes, but the principle still stands: It will

be best to consider international e-commerce as part of the overall trade system rather than a special case.

2. Make the moratorium on tariffs for electronic transmissions permanent.

The WTO moratorium on tariffs on electronic transmissions is only temporary, but should be made permanent. To ensure equal treatment between products delivered by electronic transmission (such as downloaded music) and their physically delivered counterparts (such as compact discs), tariffs should be lifted on all products with tariff-free digital counterparts.

3. Treat digitally delivered products as intangible goods.

As discussed above, a dispute exists over whether to treat downloaded products as goods or services. An agreement should be formalized to define a fully digital transaction as a service only if there is some interactive component and as an intangible good if it is developed for a mass market and sold to more than one customer. Thus, a person using the Internet to purchase and download a software application for installation on his hard drive would face the same treatment he would receive if he had the boxed copy of the software delivered to him, but a person working online interactively to develop a custom software application for a small business would face the same treatment she would receive if she visited the developer's offices.

4. Eliminate tariffs on small-value transactions.

Even with a technology solution in place to compute landed costs (total cost including all taxes, tariffs, and fees) in real time, tariffs will still act as a disincentive to international B2C transactions. Moreover, the cost of complying with customs procedures is disproportionately large on relatively small shipments. To maximize the competitive benefits of a truly global market, tariffs should be eliminated on all products, regardless of category, if the value of the transaction or the quantity of the product purchased falls below a threshold small enough to reasonably assure that the buyer is in fact the end consumer. This is simply updating the current

practice of letting consumers bring back to their own country a certain amount of goods duty free.

5. Work with third parties seeking to provide solutions.

Third parties such as SquareTrade and MyCustoms can be invaluable in facilitating international B2C transactions, but they will not succeed without the cooperation of government agencies. The MyCustoms database, for example, will be impossible to build and maintain if customs authorities do not provide timely information on tariffs and taxes. Not every third party solution will be workable or desirable, of course, but a generally cooperative attitude will promote the growth of global e-commerce over the long run.

6. Promote consumer education efforts.

No amount of public or private effort to facilitate global e-commerce will work if consumers are not confident about such transactions. All interested parties, including government agencies, should make efforts to educate consumers on the benefits and the risks of e-commerce in general, and on the specific issues involved with cross-border e-commerce. It is in everyone's best interest to inform consumers of the tools available to facilitate these transactions, the danger of making assumptions about consumer protection laws, and the steps they should take to protect themselves from bad actors.

7. Draft and enact global treaties governing criminal activity on the Internet.

Coordinated effort is required to deal with international Internet problems such as child pornography, hacking, and data havens. The Council of Europe cybercrime treaty currently under negotiation, though controversial, is an example of such an effort to deal with these issues.⁵⁴

Conclusion

The issues involved in global e-commerce are both numerous and complex. It is likely, in fact, that some of the most troublesome policy issues have yet to be considered because they cannot be foreseen, and will emerge as international e-

commerce grows. (By the same token, some of the problems we now anticipate may turn out to be non-issues.) Moreover, innovations on the Internet—both in technology and business—tend to occur much more quickly than international negotiating bodies can react; laws and regulations promulgated by relatively fast-acting national governments tend to be made obsolete within months by new innovations, and that tendency will only be worse for international policy frameworks.

Though it may seem counterintuitive, the best approach to handling these issues is to go slow

and let solutions emerge through an organic process of crisis control and trial and error. Allowing the anticipated barriers to emerge in the real world will give policymakers facts, rather than theories, on which to base their decisions, allowing for more precise actions that protect all parties while encouraging the continued growth of e-commerce in general. It will also allow policy to develop in consultation not only with academics and government officials, but with actual buyers and sellers with real-world experience and perspective on how to best deal with the problems of global e-commerce.

Endnotes

- ¹ The concept of jurisdiction varies according to context but it can be thought of in two basic ways: the question of who may be taken to court (personal jurisdiction) and the question of whose laws apply (prescriptive jurisdiction). Though the use of the Internet for cross-border transactions raises significant questions for both kinds of jurisdiction, this paper will focus on prescriptive jurisdiction—the question of whose laws should govern a given cross-border transaction.
- ² The term “balkanization” is used in this paper to denote de facto segregation of Internet content due to individual users choosing only to visit and transact with certain Web sites and services. This is distinct from balkanization of Internet infrastructure, in which certain service providers refuse to give their customers access to certain parts of the Internet by failing to negotiate interconnection agreements with other service providers.
- ³ Developing nations wishing to engage in global e-commerce face a number of unique challenges, the most important of which are limited telecommunications infrastructure and limited computer ownership, the two keys to Internet access. Investment in infrastructure and technology training will be required in many developing nations before deriving maximum economic development benefits from global e-commerce.
- ⁴ Some popular shopping “bots” include MySimon (<http://www.mysimon.com>), DealTime (<http://www.dealtime.com>), and BottomDollar (<http://www.bottomdollar.com>).
- ⁵ As the open-source software movement has proved, using the Internet for a global idea exchange can have profound tangible benefits as well.
- ⁶ For more on the use of government regulation to protect businesses against competition from electronic commerce, see PPI’s January 2001 paper, “The Revenge of the Disintermediated,” by Robert D. Atkinson.
- ⁷ In July 1999, the United States imposed 100 percent tariffs on some European products, including certain gourmet French foods, in retaliation for the European Union’s refusal (despite an adverse ruling from the WTO) to import from the United States beef that had been raised using hormones. To protest the tariffs, French farmers committed acts of vandalism against several McDonald’s restaurants in France that ranged from dumping tons of manure in a parking lot to destroying a restaurant still under construction. Protest leaders decried both McDonald’s and the WTO as tools of “American imperialism.”
- ⁸ The expansion of global e-commerce is likely to include nations that are not WTO members, but the principle remains the same for those nations as well.
- ⁹ Some governments, will seek to restrict trade in some goods and services on the grounds that such trade threatens important social or cultural values. Even if the WTO dispute resolution process finds that such a restriction is unwarranted, those governments are at any rate free to maintain the restrictions as the WTO has no independent enforcement authority and can only authorize retaliatory trade barriers against the country that loses a dispute.
- ¹⁰ Though it is probably impossible for a government to block access completely by a technically savvy individual with the proper equipment, methods do exist that would be largely effective for the bulk of the population. This is discussed in more detail in the section on Content Restrictions.
- ¹¹ <http://www.w3.org/P3P/>
- ¹² <http://www.w3.org/>
- ¹³ P3P technology refers to the software application itself; full implementation will require standardization of privacy policies and practices that can occur on a self-regulatory or governmental level. For an overview of the potential of this technology, see <http://www.cdt.org/privacy/pet/p3pprivacy.shtml>.
- ¹⁴ A list of the 100 best B2B marketplaces, as determined by the e-commerce rating site VerticalZOOM, can be found at <http://www.verticalzoom.com/top100.html>.
- ¹⁵ Not all harmful regulations would apply directly to e-commerce activities. For example, the International

A Third Way Framework for Global E-Commerce

Telecommunications Union (ITU) is considering imposing telephone-style payment regulations for international data traffic, a move that will discourage both the deployment of local Internet infrastructure and telecommunications policy reforms that will decrease Internet access costs for users. A better solution to this issue would be for nations with limited Internet backbone to expand their own infrastructure. For more on this issue, see http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp32.pdf.

- ¹⁶ For a comprehensive treatment of the numerous jurisdictional questions involved with cross-border e-commerce, see the American Bar Association's Project on Internet Jurisdiction (<http://www.abanet.org/buslaw/cyber/initiatives/jurisdiction.html>).
- ¹⁷ In fact, contradictory laws in different countries would in some cases make universal compliance impossible.
- ¹⁸ The "country of origin" rule is often equated with the "prescribed-by-seller" rule, in which the seller dictates the which laws and courts will cover the transaction (typically those of the seller's country of origin).
- ¹⁹ The Commission on Global Governance, in its November 1999 paper, "The Millennium Year and the Reform Process," declared that cyberspace requires government which is "genuinely international" (<http://www.cgg.ch/millennium.htm>).
- ²⁰ The ABA Project on Internet Jurisdiction highlights the importance of intent in determining whether a Web site targets a particular forum, but suggests that simply selling to an individual is enough to constitute targeting: "When transactions are involved, the best evidence of intent is the willingness to deal with persons in the forum state." (London Meeting Draft report, p. 30, <http://www.abanet.org/buslaw/cyber/initiatives/draft.rtf>) This is precisely what we wish to avoid since, by definition, this would constitute a burdensome and limiting country of destination rule.
- ²¹ In a working paper on "Indirect Taxes and E-commerce" (June 8, 1999) the European Commission stated, "Businesses operating in e-commerce must recognise from the outset that they will need to include in the development of their sales protocols, the ability to compute and collect taxes on the basis of the customer's location. This inescapable fact needs to be taken on board by their professional advisors and by those involved in the development of the operational systems which enable e-commerce to function." For the full document, see http://europa.eu.int/comm/taxation_customs/publications/working_doc/taxation/ecommerceEN.pdf.
- ²² Businesses could be forced to collect taxes for another nation if both nations involved entered into a mutual tax collection agreement, but such a burden should not be imposed unilaterally.
- ²³ The European Commission's document justifying the treatment of digital downloads as services can be found at <http://europa.eu.int/comm/trade/services/ecommerce/digi.htm>.
- ²⁴ This dispute is further complicated by a debate over whether payments for digital downloads of copyrighted material should be treated as business profits or royalties. The Organisation for Economic Co-operation and Development (OECD) Technical Advisory Group on Treaty Characterization of E-Commerce Payments addresses the issue at length. (http://www.oecd.org/daf/fa/treaties/treatychar_4Sept.pdf).
- ²⁵ http://www.ppionline.org/ppi_ci.cfm?contentid=621&knlgAreaID=107&subsecid=126
- ²⁶ <http://www.mycustoms.com>
- ²⁷ The penalty is one year in jail and a fine of up to \$6,173.
- ²⁸ The OECD has an extensive program to study the issue of taxation and cross-border e-commerce transactions. (http://www.oecd.org/daf/fa/e_com/e_com.htm).
- ²⁹ A buyer-based tax compliance model, of course, does not allow for realtime pricing and full payment in a single transaction, and thus would act as a de facto barrier to global e-commerce. Governments have an incentive, therefore, to make their tax and tariff collections compatible with "single payer" database systems.
- ³⁰ http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html
- ³¹ <http://www.ita.doc.gov/td/ecom/menu.html>
- ³² <http://www.squaretrade.com>
- ³³ Typically, merchants are 100 percent liable for any fraudulent credit card transaction that occurs remotely. For

more on the scope of the problem, see Julia Angwin, “Credit-Card Fraud Has Become A Nightmare for E-Merchants,” *Wall Street Journal*, September 19, 2000, p. B1.

- ³⁴ The European Union approved a rule in November 2000, commonly known as the Brussels Regulation, that allows customers in EU member nations that have disputes with e-commerce sellers in other EU nations to sue the seller in the buyer’s home country. The rule has been widely criticized for providing disincentives for small businesses to sell to customers in other European countries, a violation of the EU’s unified market principle.
- ³⁵ Buyers generally do not come with seals, leaving sellers vulnerable to buyers who do not follow through on their obligation, but their vulnerability is no greater than under the chargeback regime. Moreover, a buyer seal program could in fact be developed, perhaps along the lines of the eBay feedback ratings.
- ³⁶ OECD has put forth a set of “Guidelines for Consumer Protection in the Context of Electronic Commerce” calling for further study on jurisdiction issues and encouraging the development of alternative dispute resolution. For the full set of guidelines, see <http://www.oecd.org/publications/e-book/9300023e.pdf>. The Federal Trade Commission (FTC) has also written a comprehensive treatment of the issue, “Consumer Protection in the Global Electronic Marketplace: Looking Ahead.” (<http://www.ftc.gov/bcp/icpw/lookingahead/lookingahead.htm>). In December 2000, an international conference was held to discuss online ADR (http://www.oecd.org/dsti/sti/it/secur/act/online_trust/online_trust_workshop.htm).
- ³⁷ The Agreement allows countries to ignore the obligations they have committed to under certain circumstances, such as serious balance-of-payment problems or threats to public health. For more information on the provisions of GATS, see http://www.wto.org/english/tratop_e/serv_e/serv_e.htm.
- ³⁸ A scheduled round of negotiations on GATS is currently underway, with member nations seeking liberalization in a large number of sectors.
- ³⁹ For more information on current regulatory issues in marketing and advertising, see the Advertising Information Group notices (<http://www.aig.org>).
- ⁴⁰ The crux of the French ruling discussed above—that the U.S.-based Yahoo! must take steps to block access by French citizens—is precisely the wrong model for jurisdiction of global e-commerce. The French government has every right to forbid its citizens from buying or even viewing Nazi items for auction, but should not be able to require compliance from a company that does not target French citizens. Instead, the government might pass a law requiring all French Internet Service Providers to block out the auction section of U.S.-based Yahoo! (www.yahoo.com) while allowing the France-based Yahoo! through (www.yahoo.fr).
- ⁴¹ Virtgame.com, an Internet gambling company, has developed a system called eBorder that can determine the location of an Internet user seeking to place a wager (www.virtgame.com). After shutting down their online operations due to a broadcast licensing dispute, Canada-based iCraveTV went to work developing a technology dubbed iWall, which will enable Web servers to determine with great accuracy the physical location of users that want to watch Internet broadcasts (<http://www.icravetv.com>).
- ⁴² When Sealand was established in 1967, it was outside the limits of British territorial waters, and in 1968 the British government lost a court case attempting to assert jurisdiction over it. The territorial waters boundary has since expanded to encompass Sealand, but the British government, while refusing to recognize Sealand as a country, has maintained a hands-off stance. It is unclear whether the U.K. can reclaim the platform at this point. For a more detailed description of the founding of Sealand and the HavenCo startup, see Simson Garfinkel’s July 2000 “Wired News” article, “Welcome to Sealand. Now Bugger Off.” (http://www.wirednews.com/wired/archive/8.07/haven_pr.html)
- ⁴³ Just as governments have the power to examine mail and listen to telephone conversations if the requisite court authority is obtained and the information is collected in the prescribed manner, governments should have the same power in the Internet world.
- ⁴⁴ Technology designed to effectively filter spam may decrease the importance of this issue.
- ⁴⁵ Rep. Jim Leach, former chairman of the House Banking and Financial Services Committee, has pushed for such legislation (H.R. 4419 in the 106th Congress).
- ⁴⁶ Cuban cigars can be brought into the U.S. legally under certain limited circumstances. For more information see <http://www.customs.ustreas.gov/travel/cigars.htm>.

A Third Way Framework for Global E-Commerce

- ⁴⁷ Some sites take no responsibility for Cuban cigars that are seized by U.S. Customs, but many sites will guarantee delivery by refunding money or reshipping packages that were seized. Such guarantees can be taken as evidence that Cuban cigars can be shipped to the U.S. easily.
- ⁴⁸ An excellent summary of the WTO principles can be found at http://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm.
- ⁴⁹ <http://www.gbde.org>
- ⁵⁰ <http://www.tabd.org> (For the TABD e-commerce priorities, see <http://www.tabd.org/resources/content/apr98.html>.)
- ⁵¹ http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm
- ⁵² http://www.oecd.org/subject/e_commerce
- ⁵³ <http://www.hcch.net> (A memo of discussions relating to jurisdiction and e-commerce is available via FTP at <ftp://hcch.net/doc/jdgmpd12.doc>. The Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters is available at <http://www.hcch.net/e/conventions/draft36e.html>.)
- ⁵⁴ The latest draft of the treaty can be found at <http://conventions.coe.int/treaty/EN/cadreprojets.htm>.

About the Authors

Shane Ham is the policy analyst for the Progressive Policy Institute's Technology & New Economy Project. Previously he was a writer and segment producer for The McLaughlin Group, a public affairs television show. He also worked as a congressional analyst for two online legislative database companies, and has served on the board of directors for an e-commerce startup. Mr. Ham attended the University of Arizona in Tucson, where he studied political science and philosophy.

Robert D. Atkinson is vice president of the Progressive Policy Institute and director of its Technology & New Economy Project. Previously he served as executive director of the Rhode Island Economic Policy Council and as a senior analyst and project director at the former Congressional Office of Technology Assessment (OTA). While at OTA, he directed *The Technological Reshaping of Metropolitan America*, a report examining the impact of the information technology revolution on America's urban areas. Dr. Atkinson has a Ph.D. in City and Regional Planning from the University of North Carolina at Chapel Hill.

Acknowledgements

Though the conclusions in this report are strictly those of the Progressive Policy Institute, the authors would like to thank the following individuals for their input and assistance: Jeremy Bash, O'Melveny and Myers LLP; Tim Bennett, AeA; Paul Brownell, National Venture Capital Association; Marilyn Cade, AT&T; Glee Harrah Cady, Privada; Chris Caine, IBM; Nat Clarke, AT&T; Roger Cochetti, VeriSign; Doug Comer, Intel; Marc Cummings, Infotech Strategies; David Drake, Novartis; Claude Fontheim, Fontheim International; Mark Gitenstein, Mayer, Brown & Platt; Fred Hannett, The Capitol Alliance; Link Hoewing, Verizon; David Huang, MyCustoms; David Johnson, Wilmer, Cutler & Pickering; Hope Johnston, AT&T; Ken Levinson, Fontheim International; Cara Cherry Lisco, SquareTrade; Anne Little, SquareTrade; Michael Maibach, Intel; Dana Marshall, Verner, Liipfert, Bernhard, McPherson, and Hand; Elliott Maxwell, Aspen Institute; Mark McCarthy, VISA; Michael McShane, TRW; Peter Pitsch, Intel; Bob Rogers, Siemens Corporation; Christopher Roosa, VeriSign; Jay Rosenblum, Ernst & Young; Lisa Rosenthal, Federal Trade Commission; Anne Saunders, The Michael Lewan Company; Ari Schwartz, Center for Democracy and Technology; Tim Sheehy, IBM; Ray Strassburger, Nortel Networks; Leslie Stroh, *The EXPORTER*; Thomas Vartanian, Fried, Frank, Harris, Shriver & Jacobson; Carol Wilner, AT&T, and Andrew Wyckoff, Organisation for Economic Co-operation and Development. The authors would also like to thank their colleagues at the Progressive Policy Institute and the Democratic Leadership Council for their invaluable support and advice: Jenny Bates, Ed Gresser, Theo Yedinsky, Lisa Middlebrook, Leo Ming, Chuck Alston, and Will Marshall.