IMPEDIMENTS TO DIGITAL TRADE

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

MAY 22, 2001

Serial No. 107–36

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

72–824PS WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

NATHAN DEAL, Georgia
Vice Chairman
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ED BRYANT, Tennessee
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

EDOLPHUS TOWNS, New York
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

IMPEDIMENTS TO DIGITAL TRADE

TUESDAY, MAY 22, 2001

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 2 p.m. in room 2322, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Deal, Shimkus, Bryant, Pitts, Walden, Bass, Tauzin (ex officio), Towns, Harman, and Gordon.

Staff present: Ramsen Betfarhad, majority counsel; David Cavicke, majority counsel; Mike O'Rielly, majority professional staff; William Carty, legislative clerk; and Bruce Gwinn, minority counsel.

Mr. STEARNS. Good afternoon. The subcommittee will come to order. I want to particularly welcome all the witnesses today to the Commerce, Trade, and Consumer Protection Subcommittee hearing on digital trade.

I want to convey my special thanks to the Department of State for enabling Mr. Kovar, our Chief Negotiator at the Hague Convention, to testify today. I know you have had short notice, but I appreciate sincerely your coming. I understand the Department took on the tall order of acquiring all the requisites approval in a short period of time. This type of government agency responsiveness and efficiency is always appreciated and remembered.

I am pleased that the committee is looking at an increasingly significant component of our international trade, namely digital trade. Let me just cite to a statement that I received this morning to illustrate the importance of digital trade. The statement, part of a daily email briefing on tech issues by the Washington Association, reads, "Did you know that Forrester Research predicts worldwide Internet commerce, both business-to-business and business-to-commerce, will hit almost $7 trillion in the year 2004? North America represents a majority of this trade, but its dominance will fade as some Asian Pacific and Western European countries hit hypergrowth over the next 2 years. There is no question that as e-commerce grows digital trade, or international e-commerce, will grow even faster."

Digital trade issues raised in today's hearing, such as the Hague Convention, classification of digitally delivered products, the Safe Harbor, et cetera, are seemingly innocuous and technical in nature,

of interest to and worthy of consideration by lawyers only. But they could and do impact the growth of digital trade in profound ways.

It is incumbent on us to promote policies that advance digital trade, as it holds great promise, not just for the American economy but also the world economy as a whole. As evidenced by some of the testimony we will hear today, digital trade holds the real promise of providing people in historically underserved nations with a real chance of improving their economic standing and to do so at an accelerated pace.

But that promise is all contingent on coordinated and affirmative action on the part of the administration, Congress, and industry, making sure that forces of global protectionism and fragmentation don't take hold of digital trade. The risk of national and/or regional policies having either intended or unintended consequences stifling digital trade is ever present. Vigilance and constructive engagement on all transnational issues affecting digital trade must be maintained by all—the administration, Congress, and industry.

Our hearing today signals the subcommittee and full committee's commitment to such vigilance and constructive engagement. Mr. Kovar's efforts at the Hague is indicative of the administration's vigilance and constructive engagement. I commend the State Department for its work on the Hague Convention, and I urge greater vigilance and constructive participation by the administration in all forms, regional or multinational, where issues of import to digital trade are being considered and negotiated.

Having been in Congress for a little over 12 years, I know how difficult it is to advance a complete and public policy on a national scale of this matter. There are always differing opinions as to the best policy and, of course, differing sensitivities to the policy. So I am very mindful that in the international context any issue worth the paper it is written on is engendered with great complexity. On international matters, parties may not only have differing thoughts with respect to an issue, but those different thoughts may be driven by a completely different cultural, historic, and economic world view from ours.

With that understanding, I want to emphasize that this subcommittee's role in digital trade disputes shall be a constructive one. Constructive engagement does not, however, preclude active participation. My colleagues, we look forward to working closely with the administration and industry to advance the cause of digital trade, because it holds great promise for all of us.

Mr. Shimkus for an opening statement.

Mr. SHIMKUS. Thank you, Mr. Chairman. I am glad we have this great panel of folks to testify. I look forward to hearing—its complex issue for us simple folks from southern Illinois. I look forward to—I am having—I do have an opportunity to travel to Europe at the end of this week as part of the NATO Parliamentary Assembly that I am a member of. We will be talking some trade issues with our fellow parliamentarians that are members of the NATO Alliance.

So maybe there is something that I can learn here today and talk to some of my colleagues from our transatlantic partners that will be helpful in the discussions or at least throw something new out

on the table as far as an impediment. So I look forward to your testimony, and I yield back my time, Mr. Chairman.

Mr. STEARNS. The gentleman from New Hampshire, Mr. Bass.

Mr. BASS. Thank you very much, Mr. Chairman, and I appreciate this hearing. It is interesting; it is part of an ongoing learning curve in this what is a very complicated issue. I am looking forward to hearing from the witnesses, and I have three observations or concerns, if I may.

First, I am concerned about mechanisms that national and international law might use to compel private industry to become tax collectors for foreign nations. The positions we take on the applicability of State sales and use taxes in the U.S. may have broad implications internationally.

Second observation, I am interested in the classification of products as goods or services being dependent upon how the product is delivered. While it may be premature to consider this question, again, our answers may affect domestic policy in unintended ways.

And, last, I am interested in related jurisdictional questions regarding the location of the transaction and any involved parties, how problems ought to be mediated and, where necessary, adjudicated, and which treaty or convention describes the rules.

I look forward to hearing the testimony, and I yield back to the chairman.

Mr. STEARNS. I thank the gentleman. The gentleman from Tennessee?

Mr. BRYANT. Thank you, Mr. Chairman. I, too, appreciate your having this hearing, and I must apologize to the panelists. We are also in a concurrent meeting that will start at 2:30 for the Prescription Drug Task Force, and I am going to be moving back and forth. And I don't have any statement for the record other than as I came in I heard part of Mr. Shimkus' statement that he hoped to learn something here. Having taught him when he was at West Point, I am glad to hear he said that.

Open to learning something.

Mr. STEARNS. I thank my colleagues. Let me start by just introducing briefly the witnesses. Mr. Jeffrey Kovar, Chief U.S. Negotiator, Hague Convention, and Assistant Legal Advisor for Private International Law, U.S. Department of State. And I want to thank you for participating on one panel. My concern was we have both government and private industry on one panel only because we have so many amendments today, we are going in and out, and I thought it might be—to expedite this and at the same time allow us a forum to talk to all of you on different subjects. So I appreciate your assistance here and your patience.

Mr. George Vradenburg, executive vice president, Global and Strategic Policy, AOL/Time Warner. We have Ms. Bonnie Richardson, vice president, Trade and Federal Affairs, Motion Picture Association of America; Ms. Barbara Wellbery, partner, Morrison and Foerster; and Ms. Debra Waggoner, director, Public Policy, Corning, Inc.

Before I go, the distinguished ranking member, Mr. Towns?

Mr. TOWNS. Mr. Chairman, being that I was a little delayed, detained there, I would just put my opening statement in the record, and we just go right to the witnesses. Thank you for your courtesy.

[The prepared statement of Hon. Edolphus Towns follows:]

PREPARED STATEMENT OF HON. EDOLPHUS TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Thank you Mr. Chairman. I look forward to hearing from the panel today.

I am heartened by the committee's willingness to discuss regulatory and digital trade, and the impediments that our workers and businesses face in today's marketplace.

While there are many sides of this debate that are ripe for discussion such as consumer protection and un-metered access for internet use, my primary focus is on intellectual property—and the protection of that property from international and domestic pirates.

Intellectual Property as a traded good is one of America's greatest assets. It is protected in the Constitution and we should afford the producers of this material—software companies, record labels, artists, and motion picture studios to name a few—the same protections on an international level.

Let me be clear when I state that strong enforcement of existing copyright law is needed immediately on an international level. We here in the United States would not stand for a rogue nation to take our oil, natural gas, or precious minerals from us—that would be theft plain and simple. This is the same principle Mr. Chairman. If a customer in Hong Kong would like to listen to Al Green, watch the upcoming movie Pearl Harbor, or use Microsoft Excel, they should have to pay for it just like they would pay for a barrel of oil from West Texas or a Junior's Cheesecake from Brooklyn, New York.

Lastly Mr. Chairman, it is my hope that we can keep the internet and the companies who compete on it, free from undue trade regulations that may put our companies at competitive disadvantages over their foreign counterparts. We should allow these companies' business models to catch up with the forward moving technology.

The global economy is not coming; it is upon us and we should do everything in our power to assist our companies who are competing in this global economy.

Once again, thank you Mr. Chairman and I yield back the balance of my time.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. W.J. "BILLY" TAUZIN, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Over 300 million people around the globe are now connected to the Internet. That is up from just 56 million in January of 2000. The growth in Internet connectivity is astounding. This increased connectivity for both individuals and companies has fueled economic growth—here at home and globally. Unfortunately it has also sparked protectionist responses from countries that misunderstand the role the Internet and e-commerce can play in creating economic growth and prosperity for their people. Further, these proposed responses or regimes are often designed or created as hurried reactions by intergovernmental organizations or blocks of countries with old-style economies.

This hearing will highlight a few of the very important issues we face in today's world of digital and global trade. I would like to thank Chairman Stearns for beginning a dialogue on the fundamental issues impacting international e-commerce. Make no mistake about it: this Committee will tackle the difficult issues facing international digital trade. We plan to interact with the relevant participants in the new Administration and industry representatives to ensure that U.S. competitiveness and U.S. companies are not harmed by misguided foreign regimes. The U.S. Congress will not sit back and watch e-commerce become hostage to old modes of thinking. For instance, this hearing will examine issues relating to the WTO efforts on

classification, as well as the Hague Convention on Jurisdiction, the Council of Europe's Cyber-Crime Treaty, and the so-called "Model Contract" relating to the EU Data Protection Directive. These are illustrative of the efforts by foreign governing bodies that can have a profound impact U.S. companies and more generally, e-commerce.

The classification issue relates to the manner in which our trading partners in the WTO address digitally delivered products. Periodicals, music, movies and software no longer need to be packaged in cellophane and shipped to stores, news stands or homes. They can now be delivered over the Internet, decreasing costs and increasing convenience and efficiency. And as we see greater gains in technology it will be more than content that companies can deliver directly via the Internet.

While methods of delivery have changed, many of the products delivered have stayed fundamentally the same. For example, software packaged and purchased from a local retailer can also be purchased over the Internet and delivered directly over the Internet. The products are identical, yet a few of our trading partners have indicated a preference to classify the latter as a service rather than a good under the WTO classification system. Some have proposed a "drop it on your foot" test for goods classification. This has serious trade implications given the increased use of digital delivery for goods. It means many products currently afforded the liberal treatment of goods under GATT could be classified as services and therefore subjected to a more restrictive—and possibly discriminatory—regime under GATS. It is important that we take the lead to ensure classification remains distinct from method of delivery. The Internet should facilitate trade, not present an additional barrier.

I would also like to touch on another growing impediment to digital trade. More and more we are seeing countries or groups of nations develop legislative-like efforts which, in the context of digital trade, take on extraterritorial effects. In March we held a hearing on the EU Data Protection Directive and focused specifically on provisions of the Directive that could slow transatlantic data flows. Today we will take a closer look at the Safe Harbor and Model Contracts. Like the Directive, neither appears to comport with U.S. business practice and both ignore the benefits of information exchange. The Model Contract is particularly troubling because its provisions are much harsher than those of the Safe Harbor and have not been subject to negotiation with the United States.

The new Administration has called on the EU to slow down, review the model contract and reexamine how the EU views U.S. privacy laws. I believe that this is the correct course and I look forward to working with the new Administration on this topic.

In terms of the cyber crime treaty, many U.S. companies still see a need to address some flaws with the proposed language. These issues should be addressed. The Council of Europe should make an effort to fix the issues before the document becomes a "final" final. I welcome the new Administration's interest in working on this issue but more work seems to be necessary.

For the Hague convention on jurisdiction, much more needs to be learned before such a proposal moves forward. The U.S. government should not be pressured to sign a bad document. The State Department and others have expressed restraint regarding the convention. They have shown a willingness to address existing flaws or walk away from the process if necessary. I support this stance and I look forward to working with them on this issue.

The United States is a world leader for several reasons. Not the least of which is our ability to develop and embrace new technologies. With the advent of the rail, followed by the auto and finally the airplane, the geographical barriers to free flowing interstate commerce were all but eliminated. With the development of telecommunications, many of the same barriers were completely torn-down. We have only begun to tap into the potential benefits the Internet can offer. I suggest that our trade partners consider their long term economic development before existing trade agreements are altered to fit near term interests.

I again thank the Subcommittee Chair for having today's hearing. It signals our interest in exploring these issues to ensure that the Congress is well aware of the relevant efforts by foreign governing bodies that can and will have an impact on e-commerce.

PREPARED STATEMENT OF HON. JANE HARMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

I'd like to offer my thanks to the Chairman and Ranking Member for holding this hearing.

It is critical that the Congress—and in particular the members of this Subcommittee, which is charged with overseeing trade and commerce—thoroughly understand the impact trade regimes and regulatory environments in other countries have on our companies and our consumers.

Digital trade represents a tremendous opportunity for U.S. companies. The real growth sector in digital trade is business-to- business e-commerce. The global B2B market is expected to reach $8.5 trillion by 2005. In addition to the direct financial impact, the growth of B2B can have the broadest impact on productivity in the global economy as it allows American companies to reach customers and suppliers around the world.

But in order to realize that potential, we need to set forth new "rules of engagement" that foster global digital trade and e-commerce.

Let me lay out some of the issues that I hope the witnesses today will address.

• *What are the next steps in protecting intellectual property rights?* The Internet creates the possibility of a virtually limitless market for digital content, but it also creates the possibility that music, movies and other products can be instantly and illegally distributed to millions of people.

It seems to me that we have been seeing some progress on this issue on two fronts:

—first, technology-based responses like better "watermarking" of digital content are becoming increasingly effective and sophisticated and,

—second, more and more countries are adopting global standards like those set out in the World Intellectual Property Organization treaties that the U.S. ratified in 1998.

But clearly we have a long way to go before companies are comfortable putting their content on line and consumer demand is being met.

• *Who has jurisdiction when laws are broken over the Internet?* The Hague Convention was intended to help address this question, but concerns have been raised that it fails to adequately take e-commerce and the Internet into consideration.

• *Should the WTO classify digital trade as "goods" or "services?"* Goods receive the full protection of national treatment. Services do not. The distinction is particularly relevant to the entertainment industry, because the EU and Canada impose domestic content requirements on services, but not on goods. But most digital content falls somewhere between the two.

Is this the right time to push for digital trade to be put in one or the other category, or would it be more advantageous to see a third, hybrid category that recognizes unique digital characteristics.

• *How do to get more people around the world on-line?* Most Americans who are on-line now take flat-rate, unlimited access to the Internet for granted. We also benefit from the cheapest telephone rates in the world. Internet users in other countries pay for their access by the minute.

I am eager to hear what the witnesses have to say and I stand ready to work with you and others in the industry, with my colleagues on this Committee and in Congress, and with the Administration on shaping a trade and regulatory framework that helps put our companies at the center of a thriving international trade in digital goods and services.

Mr. STEARNS. I thank you. And, Mr. Kovar, we will start with you.

STATEMENTS OF JEFFREY D. KOVAR, CHIEF U.S. NEGOTIATOR, HAGUE CONVENTION AND ASSISTANT LEGAL ADVISOR FOR PRIVATE INTERNATIONAL LAW, U.S. DEPARTMENT OF STATE; GEORGE VRADENBURG III, EXECUTIVE VICE PRESIDENT, GLOBAL AND STRATEGIC POLICY, AOL/TIME WARNER; BONNIE J.K. RICHARDSON, VICE PRESIDENT, TRADE AND FEDERAL AFFAIRS, MOTION PICTURE ASSOCIATION OF AMERICA; BARBARA S. WELLBERY, PARTNER, MORRISON AND FOERSTER, L.L.P.; AND DEBRA L. WAGGONER, DIRECTOR, PUBLIC POLICY, CORNING, INC.

Mr. KOVAR. Thank you, Mr. Chairman, and thank you, members of the subcommittee, for inviting me to testify on behalf of the Department of State.

I would like to tell you briefly about negotiations the Department is leading at the Hague Conference on Private International Law for a Convention on Jurisdiction and the Recognition and Enforcement of Foreign Judgments. This is a project that the United States initiated in 1992 to try to level the international playing field for American litigants and fill a major gap in the legal infrastructure of the global marketplace.

The Hague Conference is the oldest organization in the world for the harmonization of private law, and it is a largely technical and

non-political forum. The U.S. is a party to several Hague Conventions in the area of judicial cooperation and in family law.

At present, there is no effective international regime for enforcing the judgments of national courts in transnational legal disputes, and the United States is a party to no regional or bilateral agreements providing the reciprocal of civil judgments. If not addressed, the widening gap between the increasingly global marketplace and the isolated national court systems could eventually have an inhibiting or distorting effect on the development of the world market.

Moreover, American litigants are generally at a disadvantage, at least vis-a-vis many of our major trading partners in developing countries. Federal and State courts in the United States have a long tradition of enforcing foreign judgments, but American judgment holders are very often not able to enjoy equal enforceability abroad.

The Hague Convention negotiations, if successfully concluded, hold out the promise of addressing these important needs. The draft convention would establish three categories of rules of jurisdiction in tort and contract for international cases. One category of rules would be required in every State that becomes a party to the convention, and your case under that rule of jurisdiction would lead to enforcement of the resulting judgment. Another category of rules would be prohibited for cases covered by the convention, even if those rules are currently provided under local law. And then the third category of rules would be local rules that fall outside of the convention, and enforcement under the convention would not be available for resulting judgments.

It is not our preference in the U.S. to link enforcement of judgments to harmonized rules of jurisdiction, but European law approaches things this way, and our allies expect to restrict some traditional U.S. practices as the cost of agreeing to enforce U.S. judgments. Because U.S. courts are already largely receptive to enforcing foreign judgments, we are left without much leverage on this point.

As you might imagine, even without considering the special jurisdictional problems raised by transactions carried out on the Internet, agreeing on a common set of jurisdictional rules that would apply in Federal and State courts in international cases poses special difficulties for the U.S.

U.S. courts determine jurisdiction based on a due process analysis, which focuses on the fairness to the defendant. Most other countries in the world, by contrast, seek to establish more objective-looking rules of jurisdiction, and the draft provisions of the convention reflect this latter approach. It is not easy to harmonize these different approaches to jurisdiction, and countries are naturally wedded to their own traditions.

On top of the traditional problems of harmonizing jurisdiction, sudden rise of electronic commerce has added immense new difficulties and uncertainties. The result has been that the 1999 preliminary draft of the convention, which is now available to everyone, is unfairly weighted against U.S. jurisdictional practices, and it doesn't adequately take into account electronic commerce and intellectual property considerations. Given these concerns, the U.S.

successfully pressed to extend the Hague negotiations from their original deadline of the fall of 2000.

The Hague Convention has held several meetings devoted to electronic commerce issues raised by the draft convention, including one meeting that focused on intellectual property concerns. International experts have been invited to participate in these meetings, and delegates have benefited from their contributions. Delegations have also convened a number of informal sessions over the last 9 or 10 months to try to prepare the ground for the next formal negotiation round, which is June 6 through 20 in the Hague. The schedule of negotiations calls for one more formal round of negotiations next year, but nothing has been scheduled yet.

Here at home, the Department of State has coordinated with the Departments of Commerce, Justice, the Federal Trade Commission, the Patent and Trademark Office, Copyright Office, and other agencies. We have also reached out to business, consumer, and legal groups engaged in these issues. Just last week we convened two public all-day sessions at the Library of Congress and the FTC to hear views from the private sector and to prepare our negotiating positions for June.

The Department believes we must take an extremely careful and deliberate approach in the Hague negotiations on issues related to the Internet. The law is in flux in the United States, and we have not found a consensus in the U.S. or elsewhere on how to proceed on these issues. As a result, we are continuing to consult widely to ensure that all the various interests are heard. We hope very much that effective solutions will emerge on the Internet jurisdiction issues, as well as on many of the other extremely difficult and controversial aspects of this draft convention.

We have a lot to gain from a successful convention, and we are trying vigorously to reach the right balance of provisions to enable us to achieve a convention to which the U.S. could become a party.

We hope, Mr. Chairman, to be able to remain in close contact with the subcommittee on these issues, and we thank you very much for the interest you have shown. I would be happy to answer any questions you might have.

[The prepared statement of Jeffrey D. Kovar follows:]

PREPARED STATEMENT OF JEFFREY D. KOVAR, ASSISTANT LEGAL ADVISER FOR PRIVATE INTERNATIONAL LAW, U.S. DEPARTMENT OF STATE

Thank you Mr. Chairman and members of the Subcommittee for inviting me to testify on behalf of the Department of State.

The Department is leading U.S. efforts at the Hague Conference on Private International Law to negotiate a Convention on Jurisdiction and the Recognition and Enforcement of Foreign Civil Judgments. The Hague project—which was undertaken at the initiative of the United States in 1992—would create harmonized rules of jurisdiction in international civil cases as well as common rules for recognizing and enforcing abroad the resulting judgments. Most foreign judgments are already recognized and enforced in the U.S. under state law, but most of our trading partners do not usually grant the same treatment to U.S. judgments. A successful convention would level the international playing field for American litigants and fill a major gap in the legal infrastructure of the global marketplace.

Although international commerce, trade, and communications are accelerating at a breathtaking pace, and the growth of the Internet promises to make boundaries less relevant for commerce, the judicial settlement of transnational disputes remains largely confined to national territories. There is no effective regime for coordinating and enforcing the work of national courts in resolving transnational legal disputes.

If this widening gap between the global marketplace and the isolated national court systems is not addressed, it could well slow progress and inhibit growth in trade.

The Hague Convention negotiations, if successfully concluded, hold out the promise of addressing this important need. In this testimony, we will provide some history and background to the Hague negotiations, including how the Convention would work, describe some of the major obstacles facing our delegation, explain how we are addressing the critical issues raised by electronic commerce, and give some sense of what we think the road ahead looks like.

BACKGROUND

The recognition and enforcement of judgments from one legal system to another has long been understood as a fundamental requirement for fully integrated markets. Thus, the framers of the U.S. Constitution included the Full Faith and Credit Clause to ensure that judgments from one state would be enforceable in every other. In the same way, as part of their movement toward a unified market several European countries concluded a convention in 1968 to provide recognition and enforcement of each other's judgments. This convention, called the Brussels Convention, became a required ticket of admission to the Common Market and then to the European Union. The Brussels Convention scheme was extended to non-EU countries in Europe in 1988 through a companion instrument called the Lugano Convention. It is now the subject of a regulation of the European Commission, scheduled to come into force in spring 2002.

For many countries the enforcement of foreign judgments is not a matter of general law but is addressed through treaties. The United States is not a party to any convention or bilateral agreement on the recognition and enforcement of foreign judgments. We made an effort to conclude a treaty with the United Kingdom in the 1970s, which failed due to opposition in the UK toward the enforcement of U.S. tort judgments in UK courts.

By contrast with the practice of most countries, however, the United States has led the way in enforcing foreign country judgments on the basis of comity. The Supreme Court embraced this approach over 100 years ago in the case of *Hilton v. Guyot,* 159 U.S. 113 (1895). The National Conference of Commissioners on Uniform State Laws then codified the common law standard in the Uniform Foreign Money Judgments Recognition Act in the 1960's, which has been adopted in about ⅔ of the states. Judgments from countries with reliable legal systems are now predictably enforceable in federal and state courts in the United States under the common law or under the Uniform Act. Although the Supreme Court in *Hilton* suggested that it was appropriate also to require a showing of reciprocity in the country where the judgment was rendered, this requirement is not included in most states' law.

Thus, while U.S. courts are perceived as the most open in the world to the recognition and enforcement of foreign civil judgments in the absence of a treaty obligation to do so, the ability of U.S. judgment holders to enforce their judgments abroad is much more problematic. Even in those countries that will, in principle, enforce foreign judgments in the absence of a treaty, the reach of U.S. long-arm jurisdiction, what they perceive to be "excessive" jury awards, and punitive damages are sometimes considered reasons not to enforce U.S. judgments. U.S. litigants deserve the same opportunity to have their judgments enforced abroad as that enjoyed by foreign litigants in the United States.

THE NEGOTIATIONS

The successful negotiation at the Hague Conference of a convention on jurisdiction and the recognition and enforcement of foreign civil judgments would be a huge step toward an international regime for enforcing foreign court judgments. The negotiations, which have been underway since 1996, involve more than 45 countries from around the world, including virtually all major U.S. trading partners. The Hague Conference is well known for producing the Conventions on Service of Process and the Taking of Evidence Abroad, Abolishing the Requirement of Legalization, and International Child Abduction to which we are a party. Moreover, the Senate has given Advice and Consent to the Hague Intercountry Adoption Convention, and Congress has enacted implementing legislation for it. The Department of State is now preparing implementing regulations prior to depositing our instrument of accession. The Hague Conference has traditionally been a professional and non-political forum of experts in the area of conflict of laws.

If successful, the Hague Jurisdiction and Enforcement of Judgments Convention would establish a regime governing jurisdiction to sue defendants from party states in tort and contract, and would improve predictability in the enforcement of the resulting judgments. However, the requirement that the Convention create uniform

rules of jurisdiction comes as a surprise to many Americans. It reflects the approach of the EU Brussels Convention and a deep-seated feeling among many other delegations that they do not wish to enforce U.S. judgments unless we make our jurisdiction practices consistent with their view of what constitutes appropriate international rules. Since litigants from most developed countries have no substantial difficulties enforcing judgments in the United States, their governments believe they have substantial negotiating leverage over us. This would perhaps not be the case if our states included reciprocity requirements in their law.

Agreeing on a rigid set of jurisdictional rules poses special difficulties for the United States. Because the Due Process Clause puts limits on the extension of jurisdiction over defendants without a substantial link to the forum, the United States is unable to accept certain grounds of jurisdiction as they are applied in Europe and other countries. For example, we cannot, consistent with the Constitution, accept tort jurisdiction based solely on the place of the injury, or contract jurisdiction based solely on the place of performance stated in the contract.

At the same time, civil law attorneys (and their clients) are profoundly uncomfortable with jurisdiction based on doing business or minimum contacts, which they believe is vague and unpredictable. They feel strongly that certain aspects of U.S. jurisdictional practice must be restricted under the Convention. Although this difference has been partially reconciled by agreement to permit some grounds of jurisdiction under national law to continue outside the Convention, critical choices and hard negotiations remain. If the Convention is to regulate jurisdiction in international litigation it must bridge vast differences in approach toward general and specialized jurisdiction among the various countries involved. It must also provide strong and clear benefits to outweigh the inevitable concerns about giving up some current litigation options in international cases.

Apart from a host of difficulties related to jurisdiction, agreement must also be reached on how to handle a wide array of other issues raised by this sweeping and ambitious project. Some of the issues include: concurrent filings in the courts of more than one state; *forum non conveniens;* provisional and protective measures; injunctions and other non-monetary judgments; punitive, non-compensatory and "excessive" damages; a lack of fairness or impartiality in the judgment court; non-application to antitrust; and scope of application to government litigation.

The fifth negotiating session in October 1999 produced a preliminary draft text, and the original schedule called for a final negotiating session in 2000. However, after extensive consultations with industry and consumer groups, the private bar, and with government litigators,[1] the Department of State concluded that this text is not close to being ratifiable in the United States and cannot be an effective vehicle for final negotiations.

Acutely aware of the need for more time, we successfully requested the Hague Conference to extend the negotiations, and to split the final session into two parts. The first session is scheduled to be held June 6-20 in the Hague. Over the last nine months we have met several times in informal sessions with key foreign government delegations and listened with them to the views of international private sector experts and non-governmental organizations. The purpose of these sessions was to prepare the way for the June meeting by seeking to find new approaches to the most difficult issues facing the negotiations. Some constructive ideas have emerged from these informal sessions, but we are still far apart on many issues. If other delegations do not begin to show more flexibility on many key provisions we will be unable to achieve a convention that could attract sufficient support in the United States.

ELECTRONIC COMMERCE ISSUES

When the Hague Convention negotiations were first proposed by the United States in 1992, and when they began four years later, no one predicted the immensely difficult issues that would suddenly arise from the explosion of electronic commerce. The result, however, has been that the Hague Convention has provided a forum to discuss at the international level the tough issues involving jurisdiction over Internet transactions. The fact that the Convention negotiators are grappling with these issues has led to intense efforts around the world to consider the prob-

[1] We have consulted with the American Bar Association, the Association of Trial Lawyers of America, the American Law Institute, the American Corporate Counsel Association, the American Society of International Law, several consumer organizations, the Maritime Law Association, trade associations and industry groups, bar associations in Chicago and New York, federal agencies with substantial litigation interests, and leading practitioners and academics. At the same time there are other groups—such as state litigating agencies and attorneys general and the banking industry—with which we have not yet been able to meet directly on the convention.

lems raised in drafting international rules of jurisdiction governing Internet transactions. In the U.S., as well, the law is in flux and courts are struggling with applying traditional U.S. jurisdiction rules to the Internet.

The Hague Conference has made an effort to facilitate the focus on electronic transactions. The Conference organized a roundtable workshop in Geneva in September 1999 and called special experts meetings in Ottawa in February 2000 and February 2001 devoted to electronic commerce issues raised by the draft Convention. Moreover, the Hague Conference arranged with the World Intellectual Property Organization to hold a special session on intellectual property issues raised by the Convention this past January, with a special focus on IP issues raised by electronic commerce.

The Department of State, working closely with the Departments of Commerce and Justice, the Federal Trade Commission, the Copyright and Patent and Trademark Offices, and other relevant agencies, has consulted closely with concerned private sector interests in the business and consumer communities on these difficult issues related to the Internet. Just last week we held two day-long public meetings at the Library of Congress and the FTC for which we had excellent attendance. We have found no consensus on the electronic commerce and intellectual property issues in the United States or elsewhere, and the Department believes we must take an extremely careful and deliberate approach in the Hague negotiations. We do not have firm views on the proper outcome of these provisions, and are seeking to ensure that all the various interests continue to be heard. We hope very much that effective solutions will emerge that will enable the Convention to move forward to a successful conclusion.

THE ROAD AHEAD

A carefully conceived and properly balanced Hague Convention would represent a tremendous opportunity for many American litigants, and we are trying vigorously to reach the right balance of provisions that would enable us to achieve a convention to which the United States could become a party. However, given the strong litigation orientation of our society and the differences between our established jurisdiction practices and those of many of the other participating countries at the Hague, the Convention negotiations present special challenges. When you add the enormous uncertainties raised by the growth of trade and commerce on the Internet and complex choices for intellectual property litigation, the obstacles can seem overwhelming. Nevertheless, the promise is great, and we hope that we can ultimately succeed.

I will be leading the U.S. delegation to next month's negotiations in the Hague. We will have a strong and diverse delegation, including members from the Departments of State, Commerce, and Justice, as well as the Federal Trade Commission, the U.S. Patent and Trademark Office, and the U.S. Copyright Office. We will also have distinguished advisers from private practice and academia, including representatives of the American Bar Association, the Association of Trial Lawyers of America, U.S. business, and U.S. consumer interests. Moreover, we expect to see private sector interests strongly represented as observers at the negotiations.

At the end of the June session decisions will be made at the Hague Conference on how to proceed. If negotiations have not been refocused in a manner that protects U.S. interests, we will evaluate our options.

When we return we will continue to reach out to as many groups, associations, and experts as we can from the private and public sector to make them aware of the draft Convention and seek their views on the opportunities and difficulties it presents for us. It is only by understanding as clearly as possible the litigation issues raised that we can be in a position to attempt to achieve a balance of provisions that could allow the United States to ratify and implement the final Convention.

We hope, Mr. Chairman, to be able to remain in close contact with the Subcommittee on these issues, and thank you very much for the interest you have shown.

Mr. STEARNS. Thank you.

Mr. Vradenburg?

STATEMENT OF GEORGE VRADENBURG III

Mr. VRADENBURG. Chairman Stearns, Mr. Towns, members of the subcommittee, I want to thank you for holding this important hearing on digital trade.

AOL/Time Warner is committed to seeing the power of information and the promise of connection brought to more people around the world in the belief that greater information and connectivity will drive individual opportunity, economic prosperity, and increased knowledge.

The dispersion of information and communications technology is driving economic development and social progress, not only here in the United States but in lesser developed nations around the world. Why is this? Because low-cost communications reduces entry barriers to businesses, particularly small and medium-sized enterprises, increases competition and innovation among sellers, creates greater choice for consumers, and enables more rapid dispersion of information.

We, as a company, want to make sure that no one is left behind in this Internet century, and universal and affordable communications and information worldwide is critical to this objective. Our ability to achieve this objective depends very much upon framing an international trade environment that will empower users worldwide to enjoy the benefits of the Internet revolution. We believe there are seven essential issues that we must tackle together to extend e-commerce and the Internet to create a global networked economy.

First and most important is a lowering of telecommunications costs. Affordability can best be assured throughout the world through privatization and competition in telecommunications services, as well as by unmetered pricing for Internet access services. Mr. Shimkus, you asked what you might deliver to our transatlantic partners. It is this: Metered or permanent pricing of Internet use is the enemy of Internet adoption and usage. If people are watching the clock, counting up fenigs or franks or whatever it is by the minute for every minute that they are online, they will be worried about large, metered monthly phone bills. They will spend less time online or they won't go online at all or let their kids go online to do such simple things as their homework.

The second critical issue is that markets for information technology products and services must be open and accessible. Particular emphasis should be placed on lowering trade barriers on high tech capital goods and consumer devices, computer software and online services so we can deliver more services to more people at a more affordable basis.

Third, we advocate clear and effective protection for intellectual property rights. Widespread investment in computer software and diverse, local cultural products and services that will drive Internet adoption and use worldwide requires that the intellectual property in these essential creative works be protected as they are in this country and to the DMCA.

Fourth, we support the free flow of goods and services across a range of sectors that make up the e-commerce value chain. This begins with lower tariffs on the goods and services that form the building blocks of the Internet architecture, but it also includes reducing barriers to advertising services, financial services, billing and payment services, distribution services, express delivery services, air transport, and customs modernization—the full range of sectors that involve the e-commerce value chain.

Fifth, governments around the world need to fashion a neutral, simple, and efficient 21st century tax collection system that works in a global networked economy. And you are absolutely right—this has to do with State and local taxation systems in this country just as it has to do with the EU VAT system in Europe.

Sixth, we must be as committed to the free flow of information and ideas as we are to the free flow of commerce. While we recognize that national security and protection of children may justify some regulation in this area, we urge that limitations on the free flow of information and ideas, just like limitations on the free flow of goods and services, be adopted only after careful consideration, lest the social and economic benefits of human exchange be lost or mitigated.

Finally, consumer confidence in the online medium must be enhanced. Here we believe that industry has and should continue to play a leadership role in developing and promulgating standards and practices in data collection and in consumer protection that will enhance consumer confidence in the online medium.

How might we effectively advance this seven-point agenda? We believe that America's digital trade agenda can best be pursued through a multilateral, regional, and bilateral approach. We are encouraged that the President has included a number of the complements of this digital trade program in his 2001 trade agenda. To pursue this agenda effectively, AOL/Time Warner believes it is important that the President and Congress agree on terms for trade promotion authority. It is equally essential that Congress continue its commitment to China's accession to the World Trade Organization. Recognizing China's importance to the growth and development of the global economy is an essential step to bringing about the truly global networked economic system I have outlined above.

The task of advancing a vision for digital trade for our Nation and for the world is daunting, but the promise in additional individual opportunity, economic prosperity, and more knowledge dispersed among more people worldwide is well worth the effort. We look forward to working with you to achieve these important goals. Thank you very much, Mr. Chairman.

[The prepared statement of George Vradenburg III follows:]

PREPARED STATEMENT OF GEORGE VRADENBURG, EXECUTIVE VICE PRESIDENT, AOL TIME WARNER

Chairman Stearns, Mr. Towns and Members of the Subcommittee. I want to thank you for holding this important hearing on digital trade issues. At AOL Time Warner, we believe that Congress and the Administration, in partnership with the US business community, should commit ourselves to advancing global economic prosperity and social progress through a trade agenda that fosters the global electronic exchange of information and commerce.

AOL Time Warner is the world's leading Internet-powered multi-media company, with a stable of brands including AOL, Warner Bros, Warner Music Group, HBO, Time Warner Cable, Time Inc. and the Turner Networks, including CNN.

In this, the Internet Century, consumers worldwide are driving the demand for greater choice and convenience. The AOL Time Warner company is committed to the proposition that new combinations of skills, technology, and talents are essential to create the innovations that will respond to this global demand. Our company is responding with new forms of content and delivery platforms, innovative services that will make new consumer devices work together seamlessly, and new means to "connect the dots" to make technology easy-to-use for consumers. We intend to bring the power of information and the promise of connection to more people around the

world. Our ability to achieve this goal depends upon working with you, your colleagues in the Congress, and the Administration to frame the international trade environment that will enable consumers to take full advantage of the Internet revolution.

We believe that there are three powerful and related trends that are fundamentally reshaping the global economy. The first is the exponential growth in connectivity resulting from increased adoption of information and communications technologies. The second is the convergence of historically distinct communications systems and consumer devices. And the third is the increasing use of electronic communications as a channel for connecting consumers and companies and driving international business and social communities. In the aggregate, these forces are accelerating the process known as globalization, a process that I believe promises economic and social benefits to consumers, workers and citizens worldwide.

Today, more than 300 million people are online. By the year 2005, more than 1 billion people will be connected to the Internet, more than 75 percent of them outside of North America. This technological transformation is creating a networked global economy that is just beginning to demonstrate that the Internet can be a powerful engine for individual opportunity, economic prosperity and social progress.

Recently, a new study done by Caroline Freund of the Federal Reserve Board and Diana Weinhold of the London School of Economics determined just how big a difference the Web has made to trade. Looking at trade flows among 56 countries from 1995 to 1999, for the first two years, they found no impact from the Net. But starting in 1997, as Web usage accelerated, they discovered that a 10 percent increase in the number of a nation's Web sites would have led to a 1 percent rise in its trade flows in 1998 and 1999. The impact was strongest for poorer countries—suggesting that nations with fewer initial trade links can reap larger relative gains from the Web, assuming they have made basic infrastructure and technology investments.

The rapid growth of Internet usage in China also demonstrates that the appetite for electronic networks as a tool for economic reform and access to information extends well beyond the so-called developed nations and is being embraced by nations and cultures that are not employing traditional notions of "capitalism" and "democracy" in their historic development.

And the benefits of electronic commerce and digitized trade extend far beyond the immediate financial gain of the participants. Perceived social and economic benefits of global electronic networks include:

- stimulating new opportunities and investments in emerging markets by reducing the costs and barriers to reaching electronic consumers in developed markets;
- extending global electronic markets to all nations and thus bringing the benefits of choice and network economies of scope and scale to all consumers;
- providing people in historically underserved nations and areas with increased access to education, health care and other public services;
- promoting greater and more rapid access to information for children of all ages and in all nations; and
- giving people everywhere the capability of promoting their local industry and cultures without losing the benefits of participation in the global economy.

These benefits create a win-win-win situation in which the same set of actions—promoting increased digital communications and trade—brings economic and social benefits to governments, industry and individuals around the world. We have an obligation to act now to deliver on the promise of these benefits, and to promote digitized trade-friendly policies with our trading partners around the world.

We all know that adoption of the capability for increased digital communications and trade around the world isn't going to happen on its own. In fact, the opposite is true: absent affirmative action on our part, global protectionism and fragmentation may take hold. If that proves to be the case, the promise of economic opportunity and broader knowledge of the world will pass too many by—the social and economic repercussions of that neglect will not only be felt in the developing world, we all will feel it.

In a world of increasing connection, our own economic and social well being is inextricably tied to the economic and social progress of other nations and peoples. A stable world order, characterized by peace and prosperity, demands that we respond to the universal yearning for economic opportunity and social connection.

The Framework for a Global Networked Society

At AOL Time Warner, we support a basic framework for a networked global society, to bring the benefits of economic and social connectivity, including economic prosperity, increased knowledge and expanded trade, to everyone. That framework should include:

- A recognition that current WTO obligations, rules, disciplines and commitments should apply to e-commerce and acknowledgement that electronically delivered goods and services should receive no less favorable treatment under trade rules and commitments than like products delivered in physical form.
- An understanding that universal and affordable access for consumers to basic and valued-added communications services is critical to expanding the reach of electronic economic opportunity.
- An appreciation that all aspects of the e-commerce value chain must be free from trade barriers in order to prevent the weakest link from breaking the benefits of the chain.
- A new approach to content development and protection that safeguards the interests of the artists, while promoting the development of local content and providing consumers with the widest array of choice.
- A commitment that no man, woman or child is left behind in the Internet age. The age where economic and social "divides" should be put behind us. The Internet offers us a new opportunity to extend economic opportunity to more people, and we, as the champions of opportunity and freedom, should grab the historic opportunity presented to us by this remarkable new technology.

The Key Issues We Must Tackle to Create the Global Networked Society

There are six key sets of issues that we must collectively tackle to ensure the creation of a global networked society.

First, and most important, is a lowering of telecommunications costs. Consumers cannot gain access to the benefits of electronic trade in commerce and ideas unless they can afford access to the basic means of connection. Affordability can best be assured through privatization and competition in telecommunications, a structure that requires independent regulation of historic monopolies to assure cost-based consumer pricing and interconnection rates. Just as important is the pricing structure used. Research, as well as common sense, tells us that metered pricing of Internet use is the enemy of Internet adoption and usage; if people are "watching the clock" while they are online, fearful of large metered monthly phone bills, they will spend less time online or won't go online at all. For that reason, we support pro-competitive telecommunications policy throughout the globe that will result in affordable pricing for Internet access to all end users.

Second, the market for information technology products and services must be more open and accessible. Ideally, we would like to see the greatest variety of information and communications devices and services available to the broadest possible audience. Particular emphasis should be on lowering tariffs on high technology goods and software so that more people in more countries can afford the technology they need to get online and companies can build the state-of -the art networks needed to bring the benefits of the Internet to all.

Third, we advocate clear and effective protection for intellectual property rights. Widespread investment in computer software and the other cultural products and services that will drive Internet adoption and use worldwide requires that those essential ingredients to a networked global economy be protected. At the same time, network operators cannot be crippled with liability for the unknowing transmission of infringing materials. Intellectual property concerns can only be addressed on a global basis—In some countries, we have made great strides in protecting intellectual property and balancing the rights and obligations of content owners and online distributors. An extension of this balance of protections in more countries, to more people, will power local cultural industries and will bring a new creative spirit to the non-English speaking Internet community worldwide.

Fourth, we support the free flow of goods and services across a range of sectors that make up the e-commerce value chain. This begins with lower tariffs on the goods and services that form the building blocks of the Internet architecture, and include reducing barriers to advertising, financial services and internet billing and payments, distribution of content—including movies and music, express delivery services and customs modernization. We must address these "barriers" to e-commerce in a holistic and comprehensive fashion. Without such a commitment, even one weak link in the e-commerce value chain can undermine the potentially explosive growth of e-commerce and productivity enhancement, new job creation and expanded consumer choice and opportunity.

Fifth, to ensure that tax policy does not impede the tremendous growth of e-commerce, governments around the world need to identify a tax collection system that maintains market neutrality while still addressing governments' legitimate need to fund public services. To ensure that these interests are balanced, tax systems should not create market distortions, discourage transacting business on the Internet or impose greater administrative burdens on

one type of supplier than on another. The goal should be to achieve a simple, efficient, and fair tax regime appropriate to a new global networked economy—a system that promotes rather than stifles free trade.

Sixth, we must be as committed to the free flow of information and ideas as we are to the free flow of commerce. Economic, social and political innovation is the product of the exchange of ideas and information. Human progress is measured not just by commerce and technology, but by innovation in the systems for economic opportunity and personal expression and understanding. We in this country will benefit by an openness to greater information from and understanding of the rest of the world, just as the remainder of the world will benefit by a greater understanding of the principles of freedom and opportunity we enjoy here. We recognize that traditional notions of national security and, protection of children among others, may provide a justification for national regulation in this area. And we believe that private sector commitments to battle child pornography, share ideas on the security of critical infrastructures and fostering local cultural diversity can assist public administrations in advancing national objectives in those areas. But we would urge that limitations on the free flow of information and ideas, just like limitations on the free flow of goods and services, should be adopted only after careful consideration, lest the social or economic benefits of human exchange not just on a local but also a global level be lost or mitigated.

Finally, consumer confidence in the online medium must be enhanced. Here we believe that industry has and should continue to play a leadership role in developing and promulgating standards and practices that will enhance consumer confidence in the online medium. Online users continue to be concerned about the privacy and security of their personal information and about the integrity of online transactions. Global business organizations, such as the Global Business Dialogue on Electronic Commerce, recognize that our online business depends on the confidence of consumers. We, and other electronic commerce businesses, have adopted world class data collection and consumer protection practices, and we are working collaboratively with governments to ensure that consumer concerns are being appropriately addressed.

The Process for Achieving a Global Networked Society

These are what I believe are the essentials of a digital trade agenda. Let me now briefly outline how we might collectively advance this agenda.

We believe that America's digital trade agenda can best be pursued through a multilateral, regional and bilateral approach. This includes pursuing initiatives through the WTO, including a possible new round of trade negotiations, and through regional venues such as the Free Trade Agreement of the Americas and APEC. Digital trade can also be advanced through bilateral initiatives.

We are encouraged that the President has included a number of the components of our digital trade program in his 2001 Trade Agenda. We urge the US government to pursue them in a comprehensive, holistic way that brings together all the critical elements needed to advance global e-commerce and trade. But merely articulating priorities and securing congressional guidance on those priorities will not be enough.

AOL Time Warner believes strongly that our ability as a nation to advance the digital trade agenda outlined above depends upon the President's having Trade Promotion Authority from the Congress. Absent a unified national commitment to a shared trade agenda, and the necessary governance mechanism to assure that the President can advance that agenda with confidence and authority, we risk losing a national opportunity of great import. We believe the time has come for the Congress and the President to collaborate closely to define trade negotiation objectives of our country and to ensure a mechanism to secure congressional approval of trade agreements that advance our trade objectives. Trade Promotion Authority provides such a tool.

TPA is much more than simply a legal tool. It is a demonstration of a shared commitment of the two branches of the US government responsible for the conduct of commerce and trade that America is ready to approach the rest of the world with a firm commitment to markets in commerce and ideas and to deliver to American consumers, farmers and businesses the economic and social benefits of a networked global economy.

It is equally essential that Congress continue its commitment to China's accession to the World Trade Organization. Recognizing China's importance to the growth and development of the global economy is an essential step to bringing about the global networked economic system that I have outlined above. We recognize that the process of WTO accession for China has proven to have taken longer than originally contemplated; we recognize that there have been significant developments in our relationship with China other than those relating to trade; but inclusion of China into

the world's trading regime remains a critical component of bringing about the full economic and social benefits of global economic and social integration.

The task of advancing a vision of digitized trade for our nation and for the world is daunting, but the opportunity—to bring additional opportunity, prosperity and knowledge to more people—is well worth the effort. We look forward to working with you to achieve this important goal.

Thank you.

Mr. STEARNS. Yes, thank you.

Ms. Richardson?

STATEMENT OF BONNIE J.K. RICHARDSON

Ms. RICHARDSON. Mr. Chairman, Congressman Towns, members of the subcommittee, thank you all for devoting your time and your attention——

Mr. STEARNS. Ms. Richardson, you might just pull the microphone up a little closer. Thanks.

Ms. RICHARDSON. [continuing] to the important issues of international trade in digital content.

I am testifying today on behalf of the Motion Picture Association of America. We represent seven of the major producers and distributors of filmed entertainment. Warner Brothers is our member, as are Universal, Fox, Sony Picture, Paramount, MGM, and the Walt Disney Company. The creative industries are America's No. 1 export industry. We earn more revenue abroad than autos and auto parts, than agriculture, than aircraft. As my boss, Jack Valenti, is fond of saying, "We are the jewel in America's trade crown." We also create jobs in the United States at three times the rate of the rest of the economy.

And our future belongs in digital content. The digital world provides exciting new opportunities for the delivery of filmed and digital entertainment, whether it is to cinemas, to home consumers, whether it is a new way of bringing television programming to consumers.

There are four issues that I would like to raise with you in my testimony today. First of all, the importance of protecting intellectual property on the Internet. Second, I would like to touch, but only briefly, on the Hague Convention, since I am surrounded by some of the world's experts on that area. I would also like to touch upon the issues of cultural diversity and cultural protectionism, and then touch briefly on the classification debate of goods versus services in the WTO and other trade contexts.

First, the intellectual property issue. As anyone who has listened to my colleagues at the Motion Picture Association could probably tell you, as well as I, Internet piracy is the single biggest threat to our industry today. That is true in the United States, and it is certainly true abroad. Piracy is not a new problem. We have spent $1 billion or more over the past 25 years in combating traditional forms of piracy. What is new is that on the Internet, piracy can happen with a speed and a scope that is really unparalleled.

There are some important new tools on how we can address these threats to our livelihood, to the protection of the content itself. First of all, at the end of 1996, the World Intellectual Property Organization, WIPO, adopted two new treaties that helped bring copyright standards into the digital age. Congress, you, in your wisdom, over 2 years ago, implemented those treaties into

U.S. law in the Digital Millennium Copyright Act. Unfortunately, many of our trading partners have not acted as swiftly. We are still six countries short of putting into place the WIPO Copyright Treaty and eight countries short internationally of the implementation of the Performances and Photograms Treaty. So one of our big objectives, and we hope to achieve it by the end of the summer, is to get those treaties into force.

There are some other ways that we are pursuing, with the help of our Government, the improvement of international standards for copyright protection. Some important work is being done in the Free Trade Agreement negotiations in this regard. And Congress, too, has supplied us with some very important tools. The IP conditionality in the GSP Program, in the Caribbean Basin Initiative, the Andean Trade Preference Act, and the Africa Growth Opportunities Act give us important way of impressing on our trading partners that these issues matter. And certainly the annual priority setting that we can do as a result of the provisions of Special 301 remain very important to highlighting this issue in international trade.

On the Hague Convention, I welcomed the words of Mr. Kovar that the e-commerce issues in the Hague Convention, as we struggle to look at the issues of jurisdiction, must be dealt with extremely carefully and deliberately. And we would agree with that. We recognize that the Hague Convention can make things better or it can make things worse. They are extremely important issues that are at stake here, and they are very complex issues, both in the copyright and in the e-commerce world.

On cultural diversity and cultural protectionism, digital networks have solved some of the old-fashioned problems. In the Old World, there just wasn't enough shelf space. There might be one cinema or one broadcaster that you could get in your hometown, and when foreign governments confronted this problem, they thought that the way to do it was to protect our country.

As we look at removing those barriers in the digital age or keeping them off in the digital age, one of the issues we can look at is the classification debate, and I am happy to answer questions in that regard in the question and answer session.

[The prepared statement of Bonnie J.K. Richardson follows:]

PREPARED STATEMENT OF BONNIE J.K. RICHARDSON, VICE PRESIDENT, TRADE & FEDERAL AFFAIRS, MOTION PICTURE ASSOCIATION OF AMERICA

I would like to commend you, Mr. Chairman, and you, Congressman Towns, and all the Members of this Subcommittee, for devoting your time and attention to the international issues confronting the content industries in the digital age.

I am testifying today on behalf of the Motion Picture Association of America. MPAA is a trade association representing seven of the major producers and distributors of filmed and digital entertainment for exhibition in theaters, for home entertainment and for television. Our members include Buena Vista Pictures Distribution, Inc. (A Walt Disney Company), Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios, Inc., and Warner Bros., a division of AOL Time Warner.

The Jewel in America's Trade Crown:

As many of you may already know, the content industries—movies, television programming, home video, music publishing, computer games and software—are America's most successful exporters. These copyright-based industries generate more revenues internationally than any other US industry—more than aircraft, more than

agriculture, more than automobiles and auto parts. We also create jobs in the United States at three times the rate of the rest of the economy. As Jack Valenti, President and CEO of the Motion Picture Association of America, is fond of saying, the copyright industries are "the jewel in America's trade crown."

Digital networks offer new opportunities for delivering our entertainment products in international markets. In the next few months, several movie studios will launch new, encrypted on-line services. No one knows today which business model, or models, will prove most successful in getting digitized entertainment content to customers, but we may start to get some answers in the next few months.

The one thing I can tell you is that all of those business models for the digital delivery of content—at home and abroad—depend on successfully protecting the content against theft.

The Importance of Protecting Intellectual Property:

Internet piracy is the single biggest impediment to digital trade today. Piracy of copyrighted materials is not a new problem. In the last quarter century, MPAA and its associated anti-piracy organizations have spent a billion dollars fighting video piracy and signal theft around the world. At present, we have anti-piracy programs in over 80 countries. What is new in the fight against piracy in the Internet era is the speed and ease with which our products can be stolen and distributed illegally over digital networks. Today, Viant (a Boston-based consulting firm) estimates that some 350,000 movies are being downloaded illegally every day. By the end of the year, they estimate that as many as one million illegal movie downloads will take place every single day. The scale of the problem is unprecedented.

We have some new tools for combating copyright theft. At the end of 1996 the World Intellectual Property Organization (WIPO) adopted two new treaties to bring copyright standards into the digital age. These treaties clarify exclusive rights in the on-line world and prohibit circumvention of technological protection measures for copyrighted works. The United States Congress implemented those treaties over two years ago in the Digital Millennium Copyright Act. Unfortunately, other countries have not acted quite as swiftly, and the treaties are still not in effect. Twenty-four countries have deposited their instruments of ratification of the WIPO Copyright Treaty; 22 countries have completed the ratification process for the WIPO Performances and Phonograms Treaty. We hope to reach the 30-country mark before the end of the summer so the treaties can enter into effect. Of course, even after the treaties enter into force, we will continue working to get *all* countries to adhere to these important principles. One of the disturbing truths in the e-commerce world is that piracy flows to the country where the levels of protection are the lowest; even the tiniest country can be the source of extraordinary levels of damage.

Meanwhile, we support the efforts of the Administration to ensure that the standards set in the WIPO treaties and the standards in the Digital Millennium Copyright Act are incorporated into free trade agreements, including those with Singapore, Chile, and the Free Trade Agreement of the Americas.

Swift and vigorous enforcement of copyright laws by countries around the globe is also essential. Tools provided by Congress for ensuring effective enforcement of intellectual property laws remain extremely important for ensuring that countries abroad provide effective enforcement against piracy. These tools include Special 301 and other trade-related legislation, including the Generalized System of Preference (GSP), the Caribbean Basic Economic Recovery Act, the Caribbean Basin Trade Partnership Act, the Andean Trade Preferences Act, and the African Growth Opportunities Act.

The Hague Convention

The Hague Convention is also attempting to tackle issues that are very important to any company that engages in international commerce. When laws are broken, which country or countries have jurisdiction over the infractions and where can the judgments be enforced? The Hague Convention is attempting to complete an international instrument to address these questions in a global fashion.

The questions of jurisdiction are especially complex in the e-commerce world. What factors should determine *where* a transaction or resulting injuries took place? Is it where the company is headquartered? Where the server is located? Where the customer is located? Does it matter whether or not the service is being advertised or directly marketed to customers in a particular country? Does the language in which the service is being offered indicate intent, or lack thereof, to conduct business in a particular country? What does it mean to "target" activities toward a particular forum, and how do U.S. notions of minimum contacts and purposeful availment work in the online environment?

Because copyright theft is such a pervasive international problem—particularly in the Internet environment—and because we rely on courts around the world to help bring pirates to justice, the copyright industries have been particularly concerned about the new rules being formulated by the Hague Convention. A common-sense convention on jurisdiction and the enforcement of foreign judgments could have some benefit to the copyright industries in confronting global infringements, and we support the United States' efforts to reach such a common-sense solution. Unfortunately, the operative draft of the Convention is painted with a broad brush that reflects the fact that much of the discussion leading up to its creation occurred before the advent of e-commerce. As a result, and by failing to squarely address the types of difficult questions I just raised, the Draft Convention in its current form threatens to do more harm than good.

Some who oppose the treaty have focused on copyright as an example of why the Draft Convention is problematic. They point to differences in national law and the possibility that a judgment rendered in a foreign country based on foreign law will be enforced in the United States. They suggest that the solution is simply to excise intellectual property issues from this agreement. We do not view this as a good solution. The fact is that today—even in the absence of a global convention on jurisdiction—U.S. companies who engage in e-commerce must deal with differences in national laws and can be called into court in a foreign country to answer for acts that reach foreign countries. (The Yahoo! case on the sale of Nazi memorabilia in France is just one example). On top of that, the U.S. is quite liberal in its recognition and enforcement of foreign judgments. This is happening today.

It is important to keep in mind that the Hague Convention doesn't try to resolve questions of substantive law. If substantive laws were the main question, copyright issues would be *easier* to address internationally than many other e-commerce related problems, such as illegal content or privacy. There is a greater degree of harmonization of copyright laws as a result of the Berne Convention and the WTO Trips agreement than is the case in many other areas of law and policy. The problem is jurisdiction: Will the Convention result in U.S. companies finding themselves subject to jurisdiction in a forum where they would not be subject to jurisdiction today, and would the Convention result in the enforcement of judgments that today would not be enforced?

These issues of jurisdiction underlie all kinds of tort actions and are of as much concern to other e-businesses as to the copyright industries. The problems cannot be resolved simply by excising intellectual property. The same questions remain with respect to cases for defamation, for hate speech, for privacy violations, for unfair trade practices, and for all other areas of non-harmonized law. We agree with others that the current Draft Convention inadequately addresses these questions, and we believe these questions must be answered with respect to all areas of the law if the Convention is to go forward.

Cultural Diversity/Cultural Protectionism:

Many countries around the world have a reasonable desire to ensure that their citizens can see films and TV programs that reflect their history, their cultures, and their languages. In the past, when their towns might have had only one local cinema and received only one or two TV broadcast signals, the motivation for foreign governments to set aside some time for local entertainment products was understandable. In today's world, with multiplex cinemas and multi-channel television, the justification for local content quotas is much diminished. And, in the e-commerce world, the scarcity problem has completely disappeared. There is room on the Internet for films and video from every country on the globe in every genre imaginable. There is no "shelf-space" problem on the net.

In addition to solving old scarcity problems, digital networks offer exciting new opportunities for producers and consumers around the globe. A consumer in small-town America with a taste for Japanese samurai films will be able to access them via his home computer. An American exchange student to Brazil will be able to continue her addiction to Brazilian soap operas after returning home—by accessing broadcasts streamed via the Internet to authorized viewers. E-commerce offers the chance to enhance the diversity of cultural exchange in a way that has never before been possible.

Because digital networks both solve the old scarcity problem and lead to exciting new opportunities for creators around the globe to reach out to new markets, local content quotas and other forms of protectionist measures are completely inappropriate in the e-commerce world. Fortunately, to date, we haven't seen any country adopt this form of market-closing measure for digitally delivered content. We hope this market will remain unfettered—and hope we can count on your support as we work with our international trade partners to keep digital networks free of cultural

protectionism. Congressional authorization of Trade Promotion Authority will also be very helpful in empowering the Administration to negotiate these commitments in the WTO and other trade agreements.

The Classification Debate:

I have been asked to address one of the more arcane issues of digital trade—whether the delivery of content of e-commerce networks should be considered trade in goods or trade in services or both. I am happy to oblige, asking your indulgence while I dive into some fairly deep and murky waters teeming with intimidating trade jargon.

First, though, I'd like to point out that this is not a new debate. Even before the e-commerce era, MPAA had one foot in the world of goods and one foot in the world of services. When we export a canister of film, we are exporting a physical product, or a *good,* that is subject to the rules of the General Agreement on Tariffs and Trade (the GATT.) However, when a motion picture company produces a new film, or a broadcaster broadcasts that film, these are services transactions subject to the rules of the General Agreement on Trade in Services (the GATS.)

Likewise, in the e-commerce world, some transactions involving the digital delivery of motion picture images are so similar to trade in goods that they clearly should benefit from the rules of GATT. Other forms of digital delivery may be more akin to a services transaction and may fall under the rules of the GATS.

Let me give you an example. If a consumer were to place a telephone order for a DVD of the film "Finding Forrester" and have a copy of that DVD delivered to his house on a UPS truck, that is a "goods" transaction. Likewise, if the same consumer ordering a copy of the same DVD on his/her computer and had the same content delivered digitally and downloaded from his computer to a write-able DVD—that is still a "goods" transaction. The only difference is that a digital network instead of a delivery van provided the transportation from the retailer to the consumer.

The classification issue is important primarily because the rules for goods in the GATT differ from the rules for services in the GATS.

GATT (rules for trade in goods):

- automatically provides national treatment on all imported goods;
- generally prohibits quotas and other forms of quantitative restrictions, [except for theatrical screen quotas, which countries may preserve]; and
- permits tariffs on imported goods; the levels of tariffs are negotiated and then "bound."

GATS (rules for trade in services):

- provide national treatment and market access on a negotiated basis sector by sector. (Unfortunately, only about 20 countries have made any commitments in audiovisual services. We hope to do improve on this in the current round of WTO services negotiations. A similar problem may exist for computer software, although more countries made more commitments in this sector.);
- permits countries that have made national treatment or market access commitments to reserve the right to continue applying some level of restrictions;
- contains a non-binding moratorium encouraging countries not to apply tariffs to e-commerce delivered services; and
- permits negotiations on s domestic regulatory issues not covered by GATT disciplines.

So, for example, if a digitally delivered DVD were exported to Europe and classified as a good, that DVD would still be subject to the existing EU tariff of 4.5%. And, we would also know that the DVD would be free of other forms of discrimination, such as local content quotas or discriminatory taxes. But, if that same digitally delivered good were classified as a service, the EU would be able under international trade agreements to adopt new quotas or discriminatory taxes—or even to raise tariffs.

The United States must ensure that digital goods retain the level of protection they currently enjoy under the GATT rules. It would be completely unacceptable if products that are currently classified as goods—motion pictures, magnetic tapes, DVDs, etc.—lost trade benefits through a re-classification process. Simply because a new delivery mechanism (digital networks) allows these products to be delivered digitally does not justify establishing new trade barriers. We can't risk opening the door to new quotas on digital products that would be illegal today under current trade rules. Trade negotiations are supposed to be trade liberalizing—they are not supposed to lead to increased trade barriers.

MPAA agrees with the position of the Administration that is it premature and unnecessary at the present time to resolve this classification question. It is premature because the business models for delivering entertainment content to consumers over

digital networks are still evolving. It is unnecessary because the rules and precedents of the GATT regarding "like products" are so clear that we are comfortable with the protection offered by the current GATT rules. We feel confident that if any country today imposed a discriminatory barrier against US films or videos or other forms of digital goods traded over digital networks, the US could successfully challenge that restriction and win in dispute settlement in the WTO.

I want to thank the members of this committee for your keen interest in the barriers that affect digital commerce. The American film, home entertainment and TV programming industry is the only industry in America today that enjoys a positive balance of trade with every country around the globe. Together with our colleagues in the music, books and software industries, we are America's leading exporter. With your continued vigilance and support, as you work with the Administration and with foreign governments, you can ensure that America's "crown jewels" continue to sparkle brightly in the digital age.

Mr. STEARNS. Ms. Wellbery?

STATEMENT OF BARBARA S. WELLBERY

Ms. WELLBERY. Thank you. Chairman Stearns, Mr. Towns, and members of the subcommittee, good afternoon. I am a partner in the law firm or Morrison & Foerster. Before joining the firm, I worked in the Department of Commerce as Counselor for Electronic Commerce to the Under Secretary for International Trade. There, I represented the Government in negotiations with the European Commission on the Safe Harbor and in other international negotiations. Since leaving the Government, I have advised clients on a variety of electronic commerce issues, including the Hague Convention and privacy.

I am pleased to have the opportunity to appear before you today to address the Hague Convention and the Safe Harbor Privacy Accord. Many in the information technology industry have serious concerns with the convention. Their core concern is that the convention would make web site operators and Internet service providers more vulnerable to lawsuits around the world and require U.S. courts to enforce the resulting the foreign judgments. This could have damaging consequences for the U.S. IT industry.

For example, the convention would allow companies to be sued around the world for claims arising out of consumer contracts. In addition, the convention would permit ISPs and web site owners to be sued anywhere in the world for all kinds of torts, including copyright infringement, privacy, defamation, and in other countries, hate speech, since the material could be accessed worldwide. And for the most part, U.S. courts would have to enforce those judgments. As a result, copyright owners could avoid the limitations on liability they negotiated with U.S. service providers under the Digital Millennium Copyright Act, by bringing suit against service providers for copyright infringement in countries that have no laws limiting service provider liability.

In addition, the convention would compound the problem created by the French Yahoo decision. There, a French court took jurisdiction and imposed penalties against Yahoo U.S., because a web site hosted by Yahoo auctioned Nazi memorabilia and was accessible to users in France. The site's content was illegal in France, yet legal in the United States. Under the convention, U.S. courts could probably still refuse to enforce such judgments on First Amendment grounds, but courts in other countries would have to enforce them.

The result could be that the Internet is reduced to the lowest common denominator where web sites avoid any but the safest content for fear of offending someone and being hailed into court. Alternatively, the Internet could be subject to as many different standards of conduct as there are countries.

Jurisdiction is an extremely difficult question in the context of electronic commerce. Simply applying the existing rules, whether they be common or civil law rules, just doesn't work. These rules turn on physical location and are limited by geographical borders. But the Internet has no borders, and e-commerce transactions provide none of the usual cues that tell parties where the other is located, the contract was negotiated or intangible goods or services delivered. It is therefore premature to freeze current jurisdictional rules in an international convention, particularly when the rules being adopted borrow heavily from the more formalistic and rigid civil law approach to jurisdiction. Those rules heighten the risks to e-commerce. While they provide certainty, they may not provide justice, since the defendant may not have had the minimum contacts with the jurisdiction where the suit is brought.

Despite the problems in the convention, I believe the U.S. Government should remain very engaged in the convention process. In that way, the U.S. Government will be able to urge a constructive, problem-solving approach to the issues raised by the convention and to ensure that the private sector is fully involved.

U.S. Government efforts to address criticisms leveled against the convention have already generated benefits. These efforts, as Mr. Kovar said, have slowed the process and have led to close consultation with all parts of the private sector. This is particularly important in the e-commerce context where technology and market applications evolve so quickly.

A similar approach was helpful in negotiations with the European Commission on the EU Privacy Directive. The U.S. and the EU have traditionally taken different approaches to privacy, but when they realized the potentially disruptive impact that the EU directive could have on trade between them, both sides recognized the need to identify common ground and develop ways to bridge those differences. The U.S. Government consulted closely with all private sector stakeholders in developing the Safe Harbor framework. Their input was invaluable in developing a workable framework for U.S. companies that as much as possible reflects actual business practices.

Thank you again for the opportunity to appear before you today, and I will be happy to answer any questions.

[The prepared statement of Barbara S. Wellbery follows:]

PREPARED STATEMENT OF BARBARA S. WELLBERY

My name is Barbara Wellbery. I am a partner of Morrison & Foerster and I practice in the firm's Washington, D.C. office. Before joining the firm in December, 2000, I served in the Career Senior Executive Service in the Department of Commerce for six and a half years, first as Chief Counsel for the National Telecommunications and Information Administration and then as Counselor for Electronic Commerce to the Under Secretary for International Trade. I have six years of experience in developing both domestic and international privacy policy. I also participated in the White House Working Group on Electronic Commerce from its inception until I left the Government. I also have extensive experience in formulating policy on other key electronic commerce issues, such as jurisdiction and consumer protection. I have

represented the U.S. Government in bilateral negotiations with the European Commission on the safe harbor privacy accord and in a variety of other bilateral and international negotiations including the Organization for Economic Cooperation and Development, and the Asia Pacific Economic Cooperation.

Since leaving the Government, I have advised U.S. multinational companies on privacy issues and on other international issues arising in the electronic commerce context. I have also been extensively involved in meetings on The Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters adopted by the Special Commission of the Hague Conference on Private International Law Hague Convention (the "Hague Convention"). I am pleased to have the opportunity to appear before you today to discuss impediments to digital trade and specifically the Hague Convention and the safe harbor privacy accord.

Introduction

The Internet is a decentralized, borderless, global medium that presents unique opportunities and challenges for both governments and businesses around the world. As a global marketplace for both commerce and ideas, it can empower citizens, democratize societies, and spur business development by providing access to a worldwide network of customers. These same attributes place a premium on a flexible legal framework that is consistent domestically and internationally, since actions taken by one government have the ability to affect the whole of the Internet. Achieving such a legal framework is a long-term process that requires continuing dialogue and diplomacy rather than confrontation, identifying common ground despite divergent interests, and building bridges instead of insisting on one way as the right way. It also requires that all private sector stakeholders be given a place at the "table" and included in the process or any resulting framework may well prove unworkable.

The safe harbor accord is often hailed for demonstrating that such an approach can work. In that instance, as discussed further below, governments worked together to find common ground. They took a constructive, problem solving approach, despite very different national privacy regimes, involved the private sector extensively, and were able to bridge their differences. It remains to be seen whether the negotiations on the Hague Convention will take a similarly constructive approach and yield similarly constructive results.

The Hague Convention

This hearing on the Hague Convention is particularly timely as the first diplomatic convention in over 18 months is scheduled to take place next month, from June 6 through June 20. The U.S. provided the original impetus for the Hague Convention, proposing it in 1992. The driving factor was the U.S. perception that U.S. courts typically enforce foreign judgments, while foreign courts often do not enforce U.S. judgments. The Hague Convention would provide international rules on jurisdiction and recognition and enforcement of foreign judgments. It concerns two aspects of jurisdiction over a foreign person or company: (i) personal jurisdiction (can the foreign defendant be sued in this court?); and (ii) enforcement (will a court in the defendant's home country recognize and enforce the court's decision?). As a formal matter, the Hague Convention does not address choice of law. As a practical matter, however, if a court does exercise jurisdiction, there is a strong likelihood that it will often find that its own law is the applicable law, because each forum applies its own conflicts of law rules. This often leads a court to apply its own law.

The current official draft of the Hague Convention, which was adopted in October 1999, has met with significant opposition in the U.S. from a variety of private sector quarters, sometimes for conflicting reasons. A great deal of the opposition stems from the very different approaches to jurisdiction taken by common law and civil law countries and the fact that the 1999 preliminary draft borrows heavily from the civil law approach to jurisdiction. At the core of the electronic commerce community's concerns is the question of when it is proper to assert jurisdiction over companies engaged in Internet activities. Electronic commerce providers fear that the jurisdictional rules contained in the Hague Convention, which would make web site operators and Internet service providers more vulnerable to lawsuits around the world, would stymie the development of electronic commerce. The more formalistic approach to jurisdiction taken in civil law countries heightens this risk.

U.S. courts focus on issues of due process—fairness to the defendant as well as to the plaintiff—and determine jurisdiction on a case by case basis. There are few rigid rules for determining jurisdiction in the U.S. It cannot be said, for example, that a consumer can always sue in his home jurisdiction. Instead, courts generally look to whether a defendant has purposefully directed, or targeted, its activities or performed some act, purposefully availing itself of the privilege of conducting busi-

ness in the forum. If so, courts conclude that the defendant has thereby invoked the benefits and protections of the forum's laws, has minimum contacts with the jurisdiction, and could reasonably have anticipated being haled into the forum. The same general approach is used to determine jurisdiction for contract actions and tort actions, as well as for actions brought by consumers against businesses.

The approach to jurisdiction in civil law countries is usually far more formalistic than the U.S. approach. For contract actions, a plaintiff can sue in the forum where the goods or services are provided unless one party to the contract is a consumer. In those cases, the consumer can sue where he resides if the defendant solicited business through advertising (such as a web site) and the consumer took steps to conclude the contract in that jurisdiction. For tort actions, plaintiffs may sue where the harmful act or omission occurred or where the injury arose. In each instance, if the relevant criteria are met, courts may not deny jurisdiction on the grounds that it would be unfair to the defendant. Although conventional wisdom holds that the civil law approach to jurisdiction provides certainty at the expense of justice, and the common law tradition provides justice at the expense of certainty, in many, but not all contexts, they lead to the same result.

Electronic commerce creates challenges for both civil and common law approaches to jurisdiction since both depend on the geographic locations of the parties and relevant events. The Internet, however, makes it difficult if not impossible to know for example where parties are located, whether one is a consumer, where the contract was negotiated, and in the case of intangible goods and services, the physical location to which they are transmitted. U.S. courts have begun to develop approaches to jurisdiction in the context of the Internet, but U.S. law on these issues continues to evolve.[1] And, although the Hague Convention applies to electronic commerce transactions and Internet service providers, it was drafted without attention to the particular jurisdictional issues raised by electronic commerce, and thus without recognition of the significant problems it poses for the Internet and electronic commerce.

I will focus on two problems the Hague Convention creates for electronic commerce and Internet service providers, which are particularly critical.[2] First, the Hague Convention would lead to increased vulnerability to tort suits for Internet service providers. (See Article 10 of the Hague Convention.) It would permit suits for all kinds of torts, including copyright infringement, privacy, defamation, and in other countries, hate speech, to be brought wherever the act or omission occurred or where the injury arose. This jurisdictional rule would allow a company with a web site to be sued, for example, for copyright infringement anywhere its web site could be accessed; an Internet service provider could be sued wherever it makes the copyrighted work available. And yet in both instances, the company may have had no contact at all with the jurisdiction in which the suit is brought.

The Hague Convention would also allow copyright owners to avoid the limitations on liability that were negotiated with U.S. service providers under the Digital Millennium Copyright Act, by bringing suit against the service provider for copyright infringement in countries that have no laws limiting service provider liability. Although as noted above, technically the choice of applicable law is independent of the choice of forum, in fact the choice of a particular forum often leads to application of that forum's laws. In addition, where the service provider had no assets in the country in which suit was originally brought, under the Hague Convention copyright owners would be entitled to enforcement in the U.S. or any other signatory country to the Hague Convention where the service provider has assets.

The Hague Convention compounds the problem created by the torts provision by establishing that courts may also exercise jurisdiction to order provisional measures,

---

[1] To determine jurisdiction and whether an online company has purposefully availed to itself of the benefits of doing business in a particular jurisdiction through its web site, U.S. courts have identified three categories of web sites (referred to as the "Zippo Continuum"). First, courts generally exercise personal jurisdiction over businesses that enter directly into contracts through the Internet with residents of the forum because in their view, purposeful availment has occurred. Second, courts decline to exercise jurisdiction where a defendant simply posts information on an Internet web site that is accessible to users in their jurisdiction. Third, occupying a gray area, are cases in which a user can exchange information with the host computer but cannot directly enter into contracts through the Internet. Many have criticized this approach as being outdated and irrelevant.

It appears now that U.S. and Canadian courts may be shifting to a new test that focuses on an effects-based approach. *See* Michael Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction,* posted at http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf.

[2] *See also* the paper entitled *Preliminary Comments on the Hague Conference on Private International Law* attached to my testimony.

such as temporary restraining orders and preliminary injunctions.[3] While the Hague Convention also limits the effect of such provisional measures to the territory of the state in which the issuing court is located, that limitation may well prove meaningless on the Internet. An injunction ordering removal of material from a web site, at least at this time, cannot be limited geographically: a temporary injunction entered by a foreign court against a U.S. company would have to be enforced by a U.S. court, despite the fact that the injunction exceeded in scope or failed to meet the criteria established by Section 512(j) of the Digital Millennium Copyright Act of 1998. Again, this would seem to undermine the carefully balanced approach struck by the Act.[4]

The torts provision could also encourage other countries to emulate a troubling trend begun by the Yahoo France decision, in which a French court exerted jurisdiction and imposed penalties against Yahoo, U.S. because the Yahoo web site was accessible to users in France. The site's content was considered illegal in France but legal in the U.S. under the First Amendment. Other foreign courts have followed suit. Recently, two courts in France and Germany held that web site publishers who published material residing on servers outside of those countries were nevertheless guilty of defamation and hate speech in Germany and France merely because the material was accessible in those countries. While surely U.S. courts would refuse to enforce such judgments on First Amendment grounds, the Hague Convention would nonetheless compound the problem. By requiring that those judgments be enforced in other countries where U.S. companies have assets, U.S. First Amendment principles could more easily be avoided. The result could be that the Internet is reduced to the lowest common denominator, where web sites avoid any but the safest content for fear of offending someone and being haled into court.

The second critical problem the Hague Convention creates is that it would subject web-based companies to suits arising out of consumer contracts anywhere in the world. It would allow a consumer to sue in his home jurisdiction so long as the defendant has directed his activities to that state (through advertising) and the consumer has taken steps necessary for the conclusion of the activity in that State.[5] The Hague Convention also limits enforcement of choice of court clauses so that they may be enforced only when they are entered into after the dispute has arisen or they allow the consumer to bring proceedings in another court. The effect would be that a business would be vulnerable to suit anywhere in the world that its web site is accessible. And, because of the close connection between choice of forum and choice of law, companies doing business on the web would not only have to anticipate being haled into court around the world but also being subjected to different and sometimes conflicting consumer protection laws around the world. The result certainly would be that companies would be reluctant to offer their goods and services over the Internet for fear of being sued anywhere in the world and subjected to the laws of more than 170 countries.[6]

If, as noted above, U.S. courts already enforce foreign judgments, why would the Hague Convention be so problematic? The reasons are fourfold. First, the statement—that U.S. courts typically enforce foreign judgments—oversimplifies the current U.S. legal situation. Foreign judgments are presumptively enforceable by U.S. courts, but that general rule is subject to certain exceptions. For example, it is well established that U.S. courts also examine, when raised by defendants, claims that a foreign court lacked personal jurisdiction. Particularly where the jurisdiction is not a common law jurisdiction, courts will apply U.S. standards of minimum contacts in determining if jurisdiction was proper. Yet, the Hague Convention would require U.S. courts to enforce foreign judgments so long as they satisfy the requisite jurisdictional tests established by the Hague Convention even where sufficient contacts do not exist.[7] Second, as noted above, efforts by U.S. courts to adapt the minimum contacts doctrine to the world of electronic commerce are still ongoing. Incor-

---

[3] *See* Article 13 of the Hague Convention.

[4] It is not clear that differences between copyright laws would rise to the type of public policy incompatibility U.S. courts would consider under Article 28(1)(f) of the Hague Convention.

[5] *See* Article 7 of the Hague Convention. Plaintiffs are considered consumers when they conclude a contract for a purpose outside their trade or profession.

[6] This discussion of the problems raised by the Hague Convention is not exhaustive. The Hague Convention also raises many other problems for electronic commerce, including problems arising out of trademark and patent suits and the relationship to other international and regional conventions.

[7] The Hague Convention allows courts to refuse to enforce another court's judgments where they result "from proceedings incompatible with fundamental principles of procedure of the State addressed,. . ." (Article 28(1)(c) of the Hague Convention). It is unknown at this time, whether the Hague Convention will lead U.S. courts to interpret procedural due process requirements differently than they now do.

porating current jurisdictional rules in the Hague Convention at this time would freeze them in place prematurely since it is not yet clear that they have fully evolved or that they work effectively in the electronic commerce context.

Third, although it can be said that U.S. courts normally enforce foreign judgments, U.S. courts have not enforced foreign judgments arising out of the kinds of cases that arise in the electronic commerce context. For example, the foreign copyright cases that have been enforced have all involved situations where the defendant also clearly had minimum contacts with the jurisdiction in which the original suit was brought. But under the Hague Convention, U.S. courts would have to enforce foreign judgments where, for example, an Internet service provider had no contacts with the jurisdiction where the suit had been brought except that a work it had transmitted could be accessed there.

Similarly, business to consumer transactions across borders were rare before the Internet. There are therefore few if any cases of foreign judgments being enforced by U.S. courts where they result from suits brought by consumers in their home court against defendants with no contacts in that jurisdiction. Finally, the principle that U.S. courts will enforce foreign judgments does not appear to be well recognized outside the U.S. and relatively few plaintiffs try to enforce foreign judgments here. That obviously would change if the Hague Convention were finalized and the U.S. were a party.

Given the many problems raised by the Hague Convention, it may be tempting to advocate that the U.S. Government absent itself from the Hague Convention. Nevertheless, based on my first hand experience in working on behalf of the U.S. Government in international fora on a variety of electronic commerce issues, I believe U.S. interests will be better served for a variety of reasons if the U.S. Government remains part of the Hague Convention process. Efforts on the Hague Convention will likely continue with or without the U.S. Government. Continued participation by the U.S. Government will allow it to influence the Hague Convention, while disengaging will not. Nor can the U.S. avoid the effects of the Hague Convention entirely if it does come into effect. At a minimum, even if the U.S. is not a signatory to the Hague Convention, foreign judgments against U.S. companies will be enforceable in other countries that are signatories to the Hague Convention.

U.S. Government efforts to address the criticisms leveled against the Hague Convention by the U.S. private sector provide a further illustration of why it is beneficial for the U.S. Government to remain engaged in the process. First, the U.S. Government succeeded in slowing down the process and was able to secure postponement of the diplomatic conference, originally scheduled for last year, to this June. The U.S. Government also takes a unique approach in consulting extensively with all aspects of the private sector, which is particularly important in the ecommerce context, where technology and market applications evolve so quickly. It was also able to persuade other delegations to hold several informal "stocktaking" meetings and to advocate successfully including private sector experts from the electronic commerce, intellectual property, consumer, and trial lawyer communities in these meetings and in focusing attention on the problems the Hague Convention raises for electronic commerce. Absent U.S. Government involvement, private sector representatives would not have been included in these meetings. These meetings produced new, informal drafts that attempt to address the concerns discussed above. (The status of these drafts is still entirely unclear; it is not known whether they or the preliminary draft adopted in 1999 will form the basis for discussion at the June diplomatic conference, nor do they resolve many of the concerns raised by the electronic commerce community.) And, the U.S. Government continues to press to ensure that both formal and informal meetings are open to private sector participants.

Therefore, in my view the better approach is for the U.S. Government to remain involved in the Hague Convention negotiating process and to continue to urge participating countries to take a constructive problem solving approach to the issues that succeeds in bridging the differences in jurisdictional approaches rather than relying so heavily on one particular legal tradition.

Safe Harbor Privacy Accord

Privacy provides another prime example of an issue that requires countries to find common ground. Enormous amounts of information are now used on a global basis. Many multinational companies ship all their human resources data to one location for record keeping, benefits, and payroll purposes. Credit card companies do the same with bankcard information for billing purposes. Credit and insurance markets increasingly operate on a global basis and require the transfer of information about individuals across borders to evaluate their creditworthiness or insurance risks. The inherently global nature of the Internet further complicates the matter. Citizens of

one country may easily visit web sites in other countries, transferring personal information across borders as they visit. But laws, which generally are limited by nations' borders, have little effect in a medium without borders. These problems are exacerbated when nation that have longstanding differences on how to protect privacy adopt very different approaches to dealing with these issues, as do the United States and the European Union (EU). Traditionally, the U.S. has relied on self-regulation and limited sector-specific legislation to protect privacy while EU countries, which view privacy as a fundamental right, have adopted broad, highly regulatory legislation that applies the same rules to all industry sectors.

Given these longstanding differences, many U.S. companies were concerned when the European Union adopted the Directive on Data Protection, which requires that Member States enact laws prohibiting the transfer of personal data to countries outside the European Union that fail to ensure an adequate level of privacy protection. U.S. companies feared that interruptions in data flows would result in the suspension of businesses. Such across-the-board interruptions could affect billions of dollars in trade each year and interfere with the multinational companies' ability to pay and manage their employees as well as with the routine activities carried out by investment bankers, accountants, and pharmaceutical and travel companies. Just the threat of action by European authorities left U.S. companies with a great deal of uncertainty, while alternative, ad hoc approaches available to satisfy the Directive's "adequacy" standard threatened to be expensive and time consuming and thus suitable for larger companies only.

In March 1998, against the backdrop of these different privacy approaches and the serious consequences that could flow from them, the United States and the EU took up the difficult challenge posed by their different approaches to privacy. The goal of the United States Government was to create easier, more streamlined option(s) for U.S. companies transferring personal information from the EU to the U.S., particularly small and medium sized companies, and to ensure the continued flow of data across borders. The EU's goal was to ensure its citizens a high level of privacy protection. From the start, both sides agreed to adopt both sets of goals. In recognition that any interruptions in transborder data transfers could have a serious impact on commerce, the EU and the U.S. began with an acceptance of their differences and developed ways to bridge those differences. Initial steps focused on identifying common ground in their different approaches on which to build a solution.

This approach led to the "safe harbor" privacy accord. The safe harbor builds on the U.S. self-regulatory approach to privacy and more closely reflects the U.S. approach to privacy. U.S. companies may decide voluntarily if they wish to adhere to the safe harbor framework. If they so decide, they will be judged "adequate," and data flows to them from Europe will continue. It thus provides yet another option for U.S. companies to meet the requirements of the EU Directive but in no way limits their choices if they wish to take another approach for complying with the Directive.

The safe harbor provides a number of important benefits to U.S. firms. Most importantly, it offers U.S. companies that receive personal information from Europe predictability and continuity as well as a more streamlined and less expensive means of complying with the adequacy requirements of the Directive. It creates a single privacy regime for U.S. companies transferring personal information from the EU to the U.S. (since all 15 Member States are bound by the safe harbor accord) and eliminates the need for prior approval to begin data transfers to the U.S. or makes such approval automatic.

Importantly, the safe harbor framework was developed by the U.S. Government in close consultation with the U.S. private sector—industry as well as privacy advocates. We posted drafts of documents for public comment fours times during the two-year negotiation and held numerous meetings with consumer advocacy and industry groups to obtain their views on the draft documents. This input was invaluable in developing a workable framework for U.S. companies, which as much as possible reflects actual business practices, yet at the same time satisfies EU privacy requirements.[8] The U.S. Government also needs to be engaged in discussions with other governments as they develop privacy legislation.

---

[8] The EU and U.S. approaches to privacy as well as the safe harbor accord are more fully discussed in a paper I wrote entitled *Bridging the Difference: The Safe Harbor and Information Privacy in The United States and the European Union.* (A copy of this paper and another paper, entitled, *European Commission's Model Contractual Clauses: Paving The Way For International Transfers Or A New Hurdle?* on the EU's model contractual clauses are attached to my testimony.)

Conclusion

If digital trade is to reach its full potential, it will require a workable legal framework that is consistent across borders. Achieving such a framework is both a long term and difficult goal, not least because we each start with the view that our own way is the right way. In addition, these ways are often deeply entrenched as a result of centuries of differing legal traditions. It seems clear that this goal will be achieved only if the U.S. Government and the U.S. private sector are deeply engaged—both in international fora and bilaterally—in discussions on the full range of issues that affect digital trade. It is also critical to achieving this goal that the U.S. Government continue to urge other governments to agree to inclusion of private sector participants in all international discussions, including treaty negotiations. Finally, all sides must be willing to work together to identify common ground and bridge the differences in their approaches.

PRELIMINARY COMMENTS ON THE HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW

The Hague Conference on Private International Law has been negotiating a Convention on jurisdiction and enforcement of foreign judgments. The purpose of the Convention is to harmonize global rules of jurisdiction and create predictable rules for the worldwide enforcement of judgments. Discussions on this Convention began before the growth of electronic commerce, and the Convention creates new challenges in the Internet age. Consequently, the Convention, as currently drafted, creates numerous areas of concern for the Internet service providers and the entire information technology ("IT") industry. A brief overview of some of the business concerns and risks posed by the draft Articles is discussed below.

Article 10—Torts

Article 10 sets forth jurisdictional rules governing where a plaintiff can sue a defendant for actions in "tort." Torts include both physical torts, such as environmental offences and products liability, and more troubling, intangible, content-related torts such as hate speech, defamation, copyright infringement, unfair competition, libel, etc. Article 10 as drafted would allow a plaintiff to bring a tort action against a defendant in any country of the world where:

(a) the act that caused the injury occurred; or

(b) in which the *injury arose* unless the defendant establishes that the person claimed to be responsible could not *reasonably have foreseen* that the act could result in an injury in that state. A plaintiff can also bring a tort action in any country in which the act or injury may occur.

The rules governing jurisdiction in the Hague Convention apply to electronic commerce. Therefore, if Article 10 became the rule, any owner of a web page or service provider could be sued in another country simply because "injury arose" there by virtue of its being accessible over the Internet. The defendant would face difficulty proving that is was not reasonably foreseeable that injury would not occur in such country. Article 10 would have damaging, unintended consequences on the U.S. IT industry:

• The torts provision would lead to increased vulnerability to tort suits for service providers. Copyright owners could bring suit against the service provider for copyright infringement in countries that have no laws limiting service provider liability. And, while the choice of forum should be independent of the choice of applicable law, in fact the choice of forum often leads to a choice of that forum's laws because each forum's courts apply their own conflicts of law rules.

The Convention would also obligate U.S. courts to enforce the resulting judgment (unless they took the view that enforcement was contrary to public policy, which they are generally reluctant to do) Copyright owners could bypass the limitations on liability they negotiated with U.S. service providers under the Digital Millennium Copyright Act. The copyright owners could establish that injury arose in any country of the world because the copyrighted work was accessible via the Internet in such country. Even if the service provider had no assets in that country, the Hague Convention would permit the copyright owner to return to the U.S. or any other signatory to the Convention and seek to have its judgment enforced against the providers' assets in such country.

• Article 10 could encourage other countries to emulate a troubling trend begun by the Yahoo France decision, in which a French court exerted jurisdiction and penalties against Yahoo U.S. because the Yahoo website was posting content that was accessible to users in France. The content was considered illegal in France and legal in the U.S. under the First Amendment. Other courts have followed suit. Recently,

two courts in France and Germany held that website publishers who published material residing on servers outside of those countries were nevertheless guilty of defamation and hate speech in Germany and France because the material was merely accessible in those countries. While surely U.S. courts would refuse to enforce such judgments on First Amendment grounds, the Convention would nonetheless compound the problem by requiring that those judgments be enforced in other countries where there might be assets. Defendants would also need to expend unnecessary resources defending such enforcement actions. First Amendment principles in the U.S. could easily be bypassed by loose rules that encourage this type of jurisdiction grab.

• All businesses could be subject to unnecessary lawsuits around the world for "torts" such as reverse domain name hijacking, unfair competition, or passing off.

Recommendation: The Convention should be modified to make clear that network operators and Internet service providers, who are providing Internet services on behalf of third parties, should not be subject to jurisdiction from the overly broad jurisdictional concepts that run throughout the Convention. Language should be added to Article 18: If an action in tort or delict is brought in the courts of a State only on the basis that the injury arose there, those courts shall not have jurisdiction over a defendant who is a service provider, when the service provider's activity in connection with the injury is a) the transmitting, routing, or providing connections for the material which is alleged to have caused the injury; b) caching carried out through an automatic process of the material which allegedly caused the injury; c) the storage at the direction of a user of the material which allegedly caused the injury; or d) the referring or linking of users to an online location or providing other information location tools containing the material which allegedly caused the injury.

Article 12—Exclusive Jurisdiction

This Article harms U.S. patent and trademark owners by permitting any court of the world to exert *exclusive jurisdiction* over any trademark or patent matter that have as their object the registration, validity, nullity or infringement of such patent and trademarks. Notably, copyrights owners successfully excluded copyrights from the scope of exclusive jurisdiction under Article 12. Article 12 encourages a "jurisdictional grab" by encouraging a party to file a suit simply by objecting to the registration or validity of a trademark or patent, and thereby grant that court exclusive jurisdiction over the dispute. For example, if company A in country A sent a cease and desist letter to company B in country B for violating its contract, company B could simply bring an action alleging that Company A's trademark in country B is invalid. The court is country B now has exclusive jurisdiction over the contract dispute and the trademark dispute. Patent and trademark rights differ in each country and are based on complicated intellectual property case law regimes. Each country that registers trademarks and patents within its own boundaries is closest to the facts and has the best expertise to resolve disputes under its own national laws. It does not make sense for countries that did not register such trademark or patent to be ruling on the infringement or validity of patents and trademarks granted by other countries.

Recommendation: As a matter of policy, trademarks and patents should be excluded from the scope of exclusive jurisdiction in Article 12. There has been some discussion in recent Hague Convention meetings about fixing Article 12 by clarifying that only the countries that granted the registration of such patents or trademarks (or is the country in which common law rights in the trademark rights arose), should have exclusive jurisdiction to resolve all trademark and patent disputes. There are still some significant questions as to whether this proposed language adequately addresses the concerns of trademark and patent owners with Article 12. This language should be studied in detail, and if questions still arise, exclusion of all intellectual property from the Convention may be the best remedy. Article 12 should also be clarified to indicate that patent and trademark infringement cannot arise in a country in the absence of the patent or trademark owner intentionally directing the industrial property through the sale of products or services to such country. In the recent Pro-C case, a Canadian court found a U.S. trademark owner liable for infringement merely because the mark was accessible to Canadian users although the defendant did not direct products or services to users in Canada.

Article 13—Provisional and Protective Measures

This Article allows any court in which "property" is located to order any provisional measures (such as injunctions), provided that the enforcement was limited to the territory of that country. For example, if a reproduction of a copyrighted work was considered "property" located in France because French citizens could access it in France, the French court could order a broad injunction forcing the defendant to stop transmitting the content in France. This article raises many of the same con-

cerns discussed with Article 12 above. In the Internet age, property can be "located" anywhere. Provisional measures that arguably are limited to the territory of one country have permanent effects on global electronic commerce. For example, in the Yahoo France case, the court ordered Yahoo U.S. to block the IP addresses of French users, even though the content is considered legal in the U.S. and there are technical problems implementing effective blocking.

Recommendation: This is exactly the type of dangerous outcome that should be avoided in the Hague Convention. The provision on provisional measures in Article 13 should be deleted or limited to tangible property only. Alternatively, if the problems with Article 10 are adequately addressed, there may be a similar resolution of the problems articulated for Article 13.

Article 7

Article sets out rules for when a consumer may sue a defendant in the courts where the consumer resides. Article 7 as drafted would allow a consumer to sue in his home jurisdiction where:

—the claim is related to the defendant's trade or profession;
—the defendant has directed his activities to that state (through means of publicity; and
—the consumer has taken steps necessary for the conclusion of the activity in that State.

Plaintiffs are considered consumers when they conclude a contract for a purpose outside their trade or profession.

Article 7 also states that choice of court clauses will be enforced only when they are entered into after the dispute has arisen or they allow the consumer to bring proceedings in another court.

• Article 7 as drafted would allow a consumer (and perhaps a business acting outside its trade or profession) to sue a business wherever their website is accessible. It adopts a country of destination approach to jurisdiction.
• The major option for addressing this problem—choice of forum clauses—would not be available until after the dispute had arisen, increasing the vulnerability of businesses to class action suits.
• It is also unclear if the choice of court provision would allow parties to designate alternative dispute resolution as an alternative to litigation.

Recommendation: The fix could be either redrafting Article 7 so that it provides for a country of origin approach or deleting the provision entirely.

Company/Association Names: AT&T, Commercial Internet Exchange (CIX), Computer & Communications Industry Association (CCIA), Verizon.

BRIDGING THE DIFFERENCE: THE SAFE HARBOR AND INFORMATION PRIVACY IN THE UNITED STATES AND THE EUROPEAN UNION

Barbara S. Wellbery [1]

INTRODUCTION

Today's information technologies allow information to be collected, compiled, analyzed, and delivered around the world more quickly and inexpensively than ever before. Where it was once difficult, time-consuming, and expensive to obtain and compile information, it is now often available with a few simple clicks of a computer mouse. This increased access to information facilitates personal and political expression as well as commerce, education, and health care.

Information technologies are transforming the face of global commerce. World trade involving information technologies and related services and products (computer software, movies, sound recordings, databases, and financial services, to name just a few) has grown rapidly in the past decade and now accounts for over $120 billion of U.S. exports alone.[2] We are now said to live in an "Information Economy."

Consumers benefit from the increased access to information. They surf the "Internet" seeking all kinds of information. Thinking of buying a house? You can shop for it on the Internet. Information is available about neighborhoods, prices, and schools; you can even take a virtual tour of the house while on-line.

---

[1] Barbara Wellbery is a partner in the Washington office of Morrison & Foerster LLP. She was previously Counsellor to the Under Secretary for Electronic Commerce in the U.S. Department of Commerce. While there, she was the chief architect and a principal negotiator of the safe harbor privacy accord between the U.S. and the European Union. The author would like to thank Rebecca Richards and Cynthia Rich for their valuable assistance on this article.

[2] Digital Economy 2000, Department of Commerce p. 53.

Companies, too, benefit. They can create new markets as the Internet allows them to reach potential customers easily and cheaply. Increased access to information about customers can reduce marketing and inventory costs, and allow better target advertising. As a result, consumer information has become a "hot" commodity.

Not surprisingly, then, there is a growing demand for all kinds of information. The great promise of the Information Age is, however, also its greatest threat. The increased market for personal information, coupled with the ability to collect and compile it easily, has led to an enormous increase in the amount of information collected about individuals as they conduct commercial transactions and cruise the Net. Banks and credit card companies maintain information on financial records, payment histories, where people shop, and what they buy. Supermarkets and other retail stores track consumer purchases using checkout scanners. As individuals peruse various sites on the Internet, mouse clicks can be tracked , so-called "cookies." Profiles can be compiled not only of what people buy, but also of what they read, their health concerns, and perhaps their political and sexual preferences as well. Thus, information technologies increase the risks to privacy exponentially.

Moreover, privacy issues are complicated by the fact that so much information is now used on a global basis. Multinational companies may ship all their personnel data to one location for record keeping, benefits, and payroll purposes; credit card companies may do the same with bankcard information for billing purposes. Credit and insurance markets increasingly operate on a global basis and may require the transfer of information about individuals across borders to evaluate their creditworthiness or insurance risks. And, the inherently global nature of the Internet further complicates the matter. Citizens of one country may easily visit web sites in other countries, transferring personal information across borders as they visit. But laws, which generally are limited by nations' borders, may have little effect in a medium without borders.

Many nations share concerns about the impact of the expansion of electronic networks on information privacy. The United States and the European Union (EU) are both addressing these concerns, but in markedly different ways. This essay briefly examines the U.S. and EU approaches to privacy, their differences and similarities, the disruptions in global commerce the differences could cause, and one solution that has been developed for bridging those differences.

THE EUROPEAN APPROACH TO PRIVACY PROTECTION

While the United States and EU generally agree on the underlying principle that individuals should have the opportunity to control the ways their personal information is used, the U.S. and the EU employ very different means to achieve this goal. The EU's approach to privacy grows out of Europe's history and legal traditions. In Europe, protection of information privacy is viewed as a fundamental, human right. The emphasis given to information privacy in Europe arises at least in part from intrusions into information privacy that were at the root of certain World War II abuses. Europe also has a tradition of prospective, comprehensive lawmaking that seeks to guard against future harms, particularly where social issues are concerned.

The EU began examining the impact of technology on society over a fifteen years decade ago; the inquiry culminated in the adoption of a directive in July 1995 specifically addressing information privacy issues. The Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and On the Free Movement of Such Data ("Directive") took effect in October 1998. Member states were required to bring into force laws, regulations, and administrative provisions to comply with the Directive by its effective date. Several have not yet done so. Presently, six of the fifteen Member States are being sued by the Commission for failure to implement measures within the deadline established by the Directive.[3]

A quick review of its basic terms makes clear that, consistent with European tradition, the Directive takes an overarching, highly regulatory and inclusive approach to privacy issues. It has two basic objectives: first, to protect individuals with respect to the "processing" of personal information (defined as information relating to an identified or identifiable natural person); and second, to ensure the free movement of personal information within the EU through the coordination of national laws (Article 1).

The scope of the Directive is extraordinarily broad. It applies to all processing of data, online and off line, manual as well as automatic, and all organizations holding personal data. It excludes from its reach only data used "in the course of purely personal or household activity" (Article 3). The Directive establishes strict guidelines for the processing of personal information. "Processing" includes any operations in-

[3] http://europa.eu.int/comm/internal—market/en/media/dataprot/law/impl.html.

volving personal information, except perhaps its mere transmission (Article 2). For example, copying information or putting it in a file is viewed as "processing." The substantive aspects of the Directive's privacy protections are based on the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted by the Organization for Economic Cooperation and Development (OECD) in 1980.

Data Quality. The Directive requires that all personal information must be processed fairly and lawfully, so that, for example, a person whose personal information is at issue knows that it is being collected and used and must be informed of the proposed uses. Furthermore, the use of personal information must be limited to the purpose first identified and to other compatible uses, and no more information may be collected than is required to satisfy the purpose of which it is collected. In other words, the theory is that if a person provides information to obtain telephone service, that information should not be used to target that person for information about vacation trips, nor should information relevant to a customer's interests in vacation trips be required to get, for instance, telephone service. Information must also be kept accurate and up to date (Article 6).

Legitimate Data Processing. The Directive sets forth rules for "legitimate" data processing. Most basically, this requires obtaining the consent of the data subject before information is processed unless specific exemptions apply (Article 7). In addition, certain information must be provided to data subjects when their personal information is processed (Article 10), such as whether they have rights to see the data, to correct any information that is inaccurate, or to know who will receive the data (Article 12).

Sensitive Data. "Sensitive" data, such as that pertaining to racial or ethnic origins, political or religious beliefs, or health or sex life, may not be processed at all unless such processing comes within limited exceptions (Article 8).

Security. The Directive requires that "appropriate technical and organizational measures to protect data" against destruction, loss, alteration, or unauthorized disclosure or access be taken (Article 17).

Data Controllers. The Directive requires those processing data to fulfill very specific requirements. Specifically, they must appoint a "data controller" responsible for all data processing, who must register with government authorities (Article 19) and notify them before processing any data (Article 18). Notification must at a minimum include: the purpose of the processing; a description of the data subjects; the recipients or categories of recipients to whom the data might be disclosed; proposed transfers to third countries; and a general description that would allow a preliminary assessment of whether requirements for security of processing have been met (Article 19).

Government Data Protection Authorities. The Directive also mandates a government authority to oversee data processing activities. Each Member State must establish an independent public authority to supervise the protection of personal data. These "Data Protection Commissions" must have the power to: (1) investigate data processing activities and monitor application of the Directive; and (2) intervene in the processing and to order the blocking, erasure, or destruction of data as well as to ban its processing. They must also be authorized to hear and resolve complaints from data subjects and must issue regular public reports on their activities (Article 28).

Transfers of Data Outside the EU. Most importantly from the U.S. perspective, the Directive requires that Member States enact laws prohibiting the transfer of personal data to countries outside the European Union that fail to ensure an "adequate level of [privacy] protection" (Article 25). Where the level of protection is deemed inadequate, Member States are required to take measures to prevent any transfer of data to the third country. Member States and their Data Protection Commissions must inform each other when they believe that a third country does not ensure an adequate level of protection.

What Constitutes Adequacy Under the Directive?

The aspect of the Directive that raises major questions for the United States and other non-EU countries is the question of what constitutes an "adequate level of (privacy) protection." The Directive provides some guidance on how adequacy is to be determined. For example, the Directive states that the adequacy of the protection offered by the recipient country shall be assessed in the light of all the circumstances surrounding a data transfer. These include: (1) nature of the data; (2) purpose and duration of the proposed processing operation; (3) country of origin or the country of final destination; (4) rules of law in force in the destination country and (5) professional rules and security measures that apply within the recipient country (Article 25). And, while there seems to be general consensus that "adequacy" means less than "equivalence," the Directive leaves unspecified the sub-

stantive rules that in fact constitute "adequacy" as well as the procedural means for achieving it.

In June 1997, the European Commission's Working party on the Protection of Individuals with Regard to the Processing of Personal Data ("Working Party") released a discussion paper entitled "First Orientations on Transfers of Personal Data to Third Countries , Possible Ways Forward in Assessing Adequacy." The Working Party paper identifies two criteria essential to a finding of adequacy , the core substantive rules and enforcement mechanisms. The substantive rules identified in the paper closely track the Directive's requirements discussed above. They include: (1) information must be processed for a particular purpose and used only insofar as its use is not incompatible with the purpose of its collection; (2) information must be accurate and up to date and not excessive in relationship to the purposes for which it is collected; (3) individuals must be provided with information about the purpose of the collection; (4) organizational and technical measures must be taken to keep the data secure; (5) data subjects must be able to obtain copies of all data and have a right to rectification if they are inaccurate, as well as to oppose processing; and (6) transfers to third countries must be restricted unless they provide an adequate level of protection. The enforcement mechanisms must provide: (1) a good level of compliance; (2) support and help to individual data subjects; and (3) appropriate redress. The Working Party Paper also recognizes that legislation is not necessary for adequate privacy protection so long as these goals are accomplished through other means.

In issuing *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive,* a more recent report issued in July 1998, the Working Party elaborated further on the criteria a self-regulatory regime had to meet to be considered adequate. First, it reiterated that the substantive rules and enforcement mechanisms identified in its July 1997 report must be met. The self-regulatory regime must also be binding for all companies or institutions to which personal data are transferred and provide for adequate safeguards if data are passed on to non-members. In addition, the privacy regime must be transparent and have mechanisms that effectively ensure a good level of compliance. Individuals must be ensured certain rights, such as easy access to an impartial and independent body to hear complaints that can adjudicate breaches of the code and provide a remedy and compensation, as appropriate. Finally, there must be a guarantee of appropriate redress in cases of non-compliance.

Neither paper issued by the Working Party, however, provides guidance on how and where an "adequate" privacy law or program in a third country might differ from the requirements of the Directive. Until the European Union actually made "adequacy" findings and there were specific examples to examine, exactly what would constitute "adequacy" under the Directive would remain unclear.

THE U.S. APPROACH TO PRIVACY PROTECTION

Legal and historical traditions have evolved quite differently in the United States than in Europe, and the United States takes a different approach to privacy issues from the EU's. The U.S. legal tradition, rooted in concerns about governmental excesses, has led to a preference for decentralized authority, a reluctance to regulate the private sector absent demonstrated need, and generally greater concern about government excess than about private sector excess. And, while the U.S. Constitution establishes certain privacy protections for individuals, such as the right to be free from warrantless searches, it does not explicitly protect *information* privacy, nor has any such right been inferred from the Constitution. In addition, a fundamental tenet of American democracy + the First Amendment to the U.S. Constitution + requires a balance between the privacy rights of individuals and the benefits that stem from the free flow of information within and across U.S. borders.

Accordingly, when the U.S. adopted a comprehensive privacy law—the Privacy Act of 1974—it governed only the Federal Government's use of citizens' personal information. Other federal privacy protection statutes apply to specific government agencies or information, such as income tax and census data. Neither federal nor state governments, however, have adopted comprehensive information privacy protections affecting private sector data use. (Some state constitutions, such as those of California, Florida, and Hawaii, explicitly set forth a right to information privacy without specifying any rights relating directly to information privacy.)

In contrast, the information privacy laws that govern the private sector in the United States were adopted either because of specific instances of abuse, perceived market failure, or because particularly sensitive information and/or groups were involved. There is also concern that information privacy issues differ so across different industry sectors that "a one size fits all" legislative approach would lack the

necessary precision to avoid interfering with the benefits that flow from the free flow of information. For that reason, too, the U.S. has adopted limited sector-specific privacy legislation. As a result, a number of statutes cover the collection and use of personal information in specific contexts, such as children's personal information, information collected by telephone and cable companies and credit bureaus, and financial, video rental and drivers' license information. A brief review of three of these statutes makes clear that privacy statutes in the U.S take different approaches and impose different schemes for protecting privacy depending on the circumstances.

Fair Credit Reporting Act

Congress enacted the Fair Credit Reporting Act (FCRA) in 1970 to deal with widespread concerns about incorrect and widely disseminated consumer credit reports. The FCRA governs disclosure of consumer credit information by credit bureaus. It starts with the premise that widespread availability of correct credit information to parties with a real need for the information will benefit the U.S. economy. For this reason, it provides consumers with a limited right to consent to the use of their personal information.

The Act imposes strict regulations on who may use the credit information and on ensuring that the information is accurate. It thus limits the disclosure of credit information to businesses with a legitimate need for the information and provides certain rights to consumers when credit information is used to deny them an important benefit. To help ensure accuracy, the Act requires that consumers have access to information maintained about them and sets out fairly prescriptive rules governing how access must be provided. The Act also requires that the recipients of credit reports be identified, prohibits the reporting of obsolete information, and provides a correction process for inaccurate or incomplete information. And, if a consumer is denied credit for personal, family, or household purposes or is denied employment and the denial is based on information in a consumer report, the entity receiving the report is required to notify the consumer and identify the credit bureau that furnished the report in question. The FCRA allocates enforcement responsibilities among a number of federal agencies, primarily to the Federal Trade Commission.

Children's Online Privacy Protection Act

In October 1998, Congress passed the Children's Online Privacy Protection Act (COPPA). The law applies to operators of commercial web sites and online services that collect or maintain information from web site or service visitors and users and prohibits the collection of information from children under the age of 13 without verifiable parental consent. It also provides for a safe harbor from privacy liability where companies adhere to a self-regulatory program approved by the Federal Trade Commission. The Federal Trade Commission, which was charged with enforcing developing regulations under the statute, issued implementing rules in April 2000.

These rules set out criteria for web site operators and online services that are targeted to children or have actual knowledge that the person from whom they seek information is a child. They require notice of what personally identifiable information is being collected, how it will be used, and whether it will be disclosed. Subject to certain exceptions, a web site must notify parents that it plans to collect information from their child and obtain parental consent before it is collected, used, or disclosed. Conditions for more than reasonably necessary information may not be placed on a child's participation in online activities. In addition, parents must be allowed to review information collected from the child, to have it deleted, and to prohibit further collection. Finally, companies must implement procedures to protect the confidentiality, security and integrity of personal information collected from children.

Financial Modernization Act

More recently, in November 1999, the President signed into law the Financial Modernization Act. The Act's primary purpose was to overhaul the U.S. laws governing the financial services industry, but the legislation also increased the level of financial privacy protections afforded to consumers. The law requires financial institutions to disclose clearly their privacy polices up front and annually, allowing consumers to make informed choices about privacy protection. Financial institutions must also inform consumers if they intend to share or sell consumers' financial data either within the corporate family or to third parties. Consumers are entitled to choice if a financial institution plans to share information with unaffiliated third parties, subject to certain exceptions. Enforcement is allocated among Federal functional regulators (for example, the Office of the Comptroller of the Currency, the Securities and Exchange Commission, and the Federal Reserve Board), the Federal

Trade Commission, and State insurance authorities. The legislation directs these agencies to prescribe regulations necessary for its implementation. Regulations have been finalized for all federal regulators. Businesses must be in full compliance by July 2001.

U.S. Self Regulatory Privacy Initiatives

Without broad, multi-sector information privacy laws, information privacy protection in the United States has in large part relied on voluntary adoption of self-regulatory codes of conduct by industry. These codes take as their point of departure the same Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted by the OECD as form the basis for the European Directive on Data Protection. As long ago as 1983, 183 U.S. companies endorsed those Guidelines. The U.S. Government has also repeatedly endorsed these guidelines, most recently in October 1998, when the Clinton Administration reiterated endorsement of those Guidelines as part of the Ministerial Declaration on the Protection of Privacy on Global Networks issued at the Ottawa Ministerial Conference.

Recent years have witnessed the growing importance of information privacy in the United States and increasing concern, from both consumers and Clinton Administration officials, about whether such privacy is sufficiently protected. This concern has led to enactment of additional sector-specific legislation. It has not, however, resulted in any significant movement toward a European type regulatory approach or law. Rather, the emphasis has been primarily on adoption and implementation of more effective self-regulatory regimes to protect privacy or on self-regulation with teeth.

Thus, when in 1997, the Clinton Administration released *A Framework for Global Electronic Commerce,* which examines the policy issues raised by the development of electronic commerce, it noted the growing concerns about information privacy and recognized that, unless they were addressed, electronic commerce would not develop to its full potential. The report specifically recognized the high value Americans place on privacy and recommended private sector efforts and technological solutions to protect privacy. The report also identified several factors suggesting that adopting comprehensive legislation could harm the development of electronic commerce at this time.

The lack of national borders on the Internet has heightened interest in self-regulation and technological solutions to problems generally and to privacy concerns specifically. On the Internet, national laws are difficult if not impossible to enforce. In addition, since the Internet and electronic commerce are still rapidly evolving, any legislated approach at best is likely to be outdated as soon as it is adopted and at worst likely to stifle further development of these media. As a result the view taken in the report is that government should be a last, not a first, resort to fix problems. Accordingly, at the time the report was issued, the President directed the Secretary of Commerce and the Director of the Office of Management and Budget to encourage private industry and privacy advocacy groups to develop and adopt effective codes of conduct, industry-developed rules, and/or technological solutions to protect privacy on the Internet.

Subsequent annual reports on electronic commerce issued by the Clinton Administration confirmed the Administration's preference for self-regulatory solutions to privacy protection. At the same time, the Clinton Administration continued to recognize that sector-specific privacy legislation may be appropriate in certain areas, such as where the information is considered highly sensitive, as is the case with children's and financial information, as discussed above. The Clinton Administration also repeatedly cautioned that if industry did not produce adequate privacy policies, government action will be needed to safeguard legitimate privacy interests.

Since the issuance of the Clinton Administration's landmark electronic commerce report in 1997, industry has undertaken concerted efforts to create effective privacy protection via self-regulation. More than 80 of the largest companies doing business on the Internet and 23 business organizations that represent thousands of other companies formed the Online Privacy Alliance (OPA) to promote privacy on-line. The Online Privacy Alliance developed Guidelines for Effective Privacy Policies, which outline protections for individually identifiable information in an on-line or electronic commerce environment. OPA has also produced guidelines for effective enforcement of these policies.

Independent third party enforcement organizations such as the *BBBOnLine,* TRUSTe, and CPA WebTrust have also been formed to provide independent third party enforcement regimes that promote compliance with information practice codes. For example, the Council of Better Business Bureaus, a well-regarded, non-profit organization that helps to resolve consumer complaints, established *BBBOnLine* as a privacy program for online businesses. Businesses joining the program may display

a seal or trust mark to notify consumers that their web sites follow fair information practices but only after they adopt privacy policies that comport with the program's fair information practice principles and complete an assessment indicating that they have implemented those policies. Members must also submit to monitoring and review by *BBBOnLine* and agree to participate in a consumer complaint resolution system. The other enforcement programs include similar requirements and also include the display of a seal or trust mark to notify consumers. More than 1950 sites carry a privacy seal from a trusted third party and more than additional 1200 sites have applied for a seal from third-party enforcement services.

In what is perhaps a uniquely American approach to self-regulation, enforcement of self-regulatory programs is backed up by Federal Trade Commission (and other federal and state agency) enforcement. Section 5 of the Federal Trade Commission Act prohibits "unfair and deceptive acts or practices" in or affecting commerce. Deceptive practices have been defined to include representations, omission, or practices that are likely to mislead reasonable consumers in a material fashion. The FTC has repeatedly used its equitable powers under Section 5 to enforce the provisions of privacy (and other self regulatory) policies against companies failing to comply with the policies they have adopted even where those policies have been adopted voluntarily. The operational effect of these unfair and deceptive statutes is to make adoption by a company of a privacy policy akin to adoption of a privacy law for that particular company.

The FTC Act provides the FTC with authority to seek injunctive relief against future violations of the statute as well as to provide redress for injured consumers. And, the FTC can obtain substantial penalties where its orders are violated. The FTC's (and other federal and state agencies') unfair and deceptive authority and willingness to use this authority to enforce self-regulatory policies helps to ensure the effectiveness of self-regulation in the U.S. All fifty states plus the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted laws similar to the Federal Trade Commission Act to prevent unfair or deceptive acts. These are enforced by their Attorneys General, adding additional resources to government enforcement of self-regulation.

Evidence now exists that shows the United States' decentralized, self-regulatory approach to privacy issues can be an effective means of ensuring that individuals' personal information is adequately protected in a globally networked environment. A 1999 Federal Trade Commission survey involving a random sample of web sites found that the number of privacy policies had risen from 14% in 1998 to 88% and that 100% of the most popular group of web sites now have privacy policies. While only 8% of the random sample had privacy seals from one of the independent third party enforcement groups, 45% of the most popular group did. Other surveys also show that privacy self-regulation is working and that businesses are taking effective steps to establish and post privacy policies. For example, a Jupiter Communications study determined that 70 percent of web sites in the United States that collect information post a privacy policy linked to their home pages.

At the same time, there have been increasing calls for privacy legislation in the U.S. In May, 2000, the Federal Trade Commission called for legislation to protect privacy online based upon its most recent report, which identified problems of "free riders" and poor quality privacy policies. The report stated that the number of web sites disclosing information practices had increased, but that the quality of these information practices fell short. In addition, the report noted that while the creation of the self-regulatory enforcement programs has been a positive development, the number of participants to date in these groups has been relatively small (8% of a random sampling and 45% of the most popular sites). In part because these enforcement programs have not been widely implemented, the FTC has concluded that such efforts alone are not sufficient for ensuring adequate protection of consume privacy online.

Several members of Congress have also introduced privacy legislation in Congress to protect privacy, particularly in the areas of online privacy, electronic surveillance, and medical and financial record-keeping. While many of these bills are given little chance of passage, at a minimum they indicate impatience with the pace of adoption and dissatisfaction with the quality of private sector codes of conduct. For example, in the first few months of this year alone, there have been at least 18 bills proposing privacy legislation These have ranged from the basic requirements that disclosure must be provided with an opportunity to prohibit further interaction to more stringent bills requiring affirmative consent in advance to collect and disclose personally identifiable information. Even some industry officials are, for the first time, urging Congress to pass limited privacy laws. They are concerned that the lack of federal standards will lead to a confusing patchwork of state regulations.

For its part, the Clinton Administration saw substantial progress being made by the private sector, although it too believed more needed to be done and more quickly. The new Administration, however, has yet to articulate its policies in this area and whether it will also encourage adoption by industry of effective privacy policies and technological solutions.

Although the privacy situation in the U.S. is evolving, this much is clear. While the U.S. is committed to ensuring personal privacy, it does through a variety of means that reflect its deeply rooted tradition of enhancing the free flow of information and avoiding unnecessary government intervention in private affairs. In the first instance, the U.S relies on private sector self-regulatory efforts backed up by government enforcement to ensure that companies implement their privacy policies. The government gets involved only where it determines that the privacy rights of individuals are not otherwise being sufficiently protected. The U.S. approach to privacy relies on an amalgam of laws, codes of conduct, and technology to provide effective privacy protection.

Given U.S legal traditions and history and the advantages of a self-regulatory approach to privacy in an information economy, the United States is unlikely at this time to abandon its self-regulatory approach to privacy issues. And even if it were to adopt privacy legislation in new and different situations, it is highly unlikely that the United States would adopt the type of overarching, comprehensive, highly regulatory and centralized approach to privacy that the European Union has adopted.

SAFE HARBOR

Neither the EU or the U.S. appears likely to change significantly its approach to privacy protection. Given these longstanding differences, many U.S. organizations were concerned about the impact of the "adequacy" standard on personal data transfers from the European Community to the United States. Many feared an across the board interruption in data flows. Such across the board interruptions could affect as much as $120 billion in trade each year and interfere with multinational companies' ability to pay and manage their employees and with the routine activities carried out by investment bankers and accountants and by pharmaceutical and travel companies. Others dismissed fears of a complete interruption in data flows as unlikely, pointing out that it would be potentially devastating for both economies.

The more likely situation—of limited data flow interruptions involving one industry sector or perhaps one company—posed similar dangers, however, since it was feared they could easily evolve into a trade war, depending on U.S. reactions and European counter reactions. And, just the threat of action by European authorities left U.S. companies with a great deal of uncertainty. Alternative, ad hoc approaches available to satisfy the Directives "adequacy" standard threatened to be expensive and time consuming and thus suitable for larger companies only.

Against the backdrop of these different privacy approaches and the serious consequences that could flow from them, the United States and the EU took up the difficult challenge of bridging the differences in their respective approaches to privacy. Toward that end, in March, 1998 the U.S. Department of Commerce initiated a high-level informal dialogue with the European Commission Directorate for Internal Markets to ensure the continued free flow of data. From the start, both sides recognized that any interruptions in transborder data transfers could have a serious impact on commerce between the EU and the US, and that they thus needed to begin with an acceptance of their differences and develop ways to bridge those differences. At the outset, therefore, the two sides agreed on twin goals—of maintaining data flows between the U.S. and EU while maintaining high standards of privacy protection and worked to identify common ground on which to build a solution. The dialogue revealed that there is much common ground between the two sides on what constitutes effective privacy protection. Both the U.S. and the European approaches, despite their differences, are based on the 1981 OECD Privacy Guidelines.

This dialogue led in late 1998 to a proposal of a "safe harbor" for U.S. companies that adhere to a certain framework, the so-called safe harbor framework. The safe harbor framework encompasses the safe harbor principles and frequently asked questions (FAQs). U.S. companies adhering to the framework will be judged adequate and data flows to them from Europe will continue. The safe harbor principles more closely reflect the U.S. approach to privacy, but at the same time would meet the European Union Privacy Directive's requirements. The FAQs were developed to provide further guidance to U.S. companies and to elaborate on how various issues, such as enforcement, will work. Both the principles and FAQs were developed in close consultation with the European Commission and the U.S. public and both are considered integral to an "adequacy" determination. Drafts of documents were posted for U.S. public comment fours times during the two-year negotiation, and numer-

ous meetings were held by U.S. negotiators with consumer advocacy and industry groups to obtain their views on the draft documents.

Importantly, the dialogue also led to a standstill between the U.S. and the EU in late 1998. The EU made a political commitment to the U.S. not to interrupt data flows while the dialogue proceeded in good faith.

On March 14, 2000, the Department of Commerce and the European Commission announced that they had reached a tentative conclusion to the safe harbor dialogue. At the same time, the two sides agreed to continue their discussions with respect to the financial services sector, given the recent passage of the Financial Modernization Act and the fact that the regulations had not yet been issued. On May 31, the EU Member States voted unanimously to approve the safe harbor arrangement

The safe harbor will provide a number of important benefits to U.S. firms. Most importantly, it will provide predictability and continuity for U.S. companies that receive personal information from Europe. All 15 Member States will be bound by the European Commission's finding of adequacy. The safe harbor also streamlines the bureaucratic burdens imposed by the Directive, by creating one privacy regime applicable to U.S. companies, rather than 15. It also eliminates the need for prior approval to begin data transfers to the U.S. or makes such approval automatic. The safe harbor offers a simpler and less expensive means of complying with the adequacy requirements of the Directive, which should benefit all U.S. companies and particularly small and medium enterprises.

An organization's decision to enter the safe harbor is entirely voluntary. An organization that decides to participate in the safe harbor, however, must publicly declare in its published privacy policy statement that it adheres to the safe harbor and then it must do so. To continue to be assured of safe harbor benefits, an organization needs to self certify annually to the Department of Commerce in writing that it adheres to the safe harbor's requirements. The Department of Commerce will maintain a list of all organizations that file self-certification letters and make both the list and the self-certification letters publicly available.

Safe Harbor Requirements

Organizations must comply with seven privacy principles and the FAQs to be compliant with the safe harbor.[4] The principles require the following:

Notice. Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers for limiting its use and disclosure.

Choice. Organizations must give individuals the opportunity to choose (opt out) whether their personal information may be disclosed to a third party or to be used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

Onward Transfer (Transfers to Third Parties). Where an organization wishes to transfer information to a third party that is acting as an agent[5], it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

Access. Generally, individuals must be given access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate. Exceptions to this general rule are permitted where the burden or expense of providing access would be disproportionate (unreasonable) to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Security. Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

---

[4] The principles, frequently asked questions and answers, as well as other safe harbor documents can be located at www.export.gov/safeharbor.

[5] It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

Data Integrity. Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Enforcement. Organizations must have readily available and affordable independent recourse mechanisms that allow each individual's complaints to be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide. In addition, the organization must establish procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented. Finally, the organization must remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization.

The FAQs provide further guidance that clarifies and supplements the safe harbor principles on issues such as access, publicly available information, and public record information as well as sector-specific guidance for information processing by medical, pharmaceutical, travel, and accounting firms. They also address how human resources information will be handled under the safe harbor.

Safe Harbor Enforcement

Perhaps the most difficult difference to bridge in the safe harbor dialogue was the issue of enforcement. While the EU's Working Group had already determined in the abstract that self regulation was a valid means to "adequacy," accepting the adequacy of a particular self-regulatory enforcement regime proved far more difficult. Adding to this difficulty, was the complexity of the multi-layered approach to privacy enforcement in the U.S., which relies on self-regulation, backed up by FTC enforcement, sector specific laws, and recourse to lawsuits.

Ultimately, an understanding was reached on an enforcement arrangement. In general, enforcement of the safe harbor will take place in the United States in accordance with U.S. law and will be carried out primarily by the private sector. The safe harbor provides for at least three different ways to satisfy the enforcement principle. An organization can join a self-regulatory privacy program that adheres to the safe harbor's requirements. It can also develop its own self-regulatory privacy policy that conforms to the safe harbor. And, an organization can meet the safe harbor enforcement principle's requirements if is subject to a statutory, regulatory, administrative or other body of law (or rules) that effectively protects personal privacy.

As part of their safe harbor obligations, organizations are required to make available a dispute resolution system that will investigate and resolve individual complaints and disputes and procedures for verifying compliance. They are also required to remedy problems arising out of a failure to comply with the principles. Sanctions must be severe enough to ensure compliance by the organization; they must include publicity for findings of non-compliance and deletion of data in certain circumstances. They may also include suspension from membership in a privacy program (and thus effectively suspension from the safe harbor) and injunctive orders.

As noted above, the dispute resolution, verification, and remedy requirements can be satisfied in different ways. For example, an organization could comply with a private sector developed privacy seal program that incorporates and satisfies the safe harbor principles. If the seal program, however, only provides for dispute resolution and remedies but not verification, then the organization would have to satisfy the verification requirement in an alternative way. Organization can also satisfy the dispute resolution and remedy requirements through compliance with government supervisory authorities or by committing to cooperate with data protection authorities located in Europe.

Where an organization relies on self-regulation to ensure privacy protection under the safe harbor, there must be a U.S. agency (state or federal) with jurisdiction over the organization that will enforce the safe harbor policies against that organization. The agency must also be willing to take action under federal or state law prohibiting unfair and deceptive acts where the company fails to comply with the safe harbor or the organization is not eligible to join the safe harbor. Depending on the industry sector, the Federal Trade Commission, comparable U.S. government agencies, and/or the states will provide overarching government enforcement of the safe harbor principles. An annex to the safe harbor principles will contain a list of U.S. enforcement agencies recognized by the European Commission. Third party self regulatory programs, (such as BBB On-line, TRUSTe, and WEBTrust) are also subject to enforcement under these unfair and deceptive practice statutes in many if not most instances if they claim to be enforcing the safe harbor framework for their safe harbor members but do not.

Failure to Comply with Safe Harbor Requirements

If an organization persistently fails to comply with the safe harbor requirements, it will no longer be entitled to benefit from the safe harbor. Persistent failure to comply arises where an organization refuses to comply with a final determination by any self regulatory or government body or where such a body determines that an organization frequently fails to comply with the requirements to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001). The Department of Commerce will indicate on the public list it maintains of organizations self certifying adherence to the safe harbor requirements any notification it receives of persistent failure to comply and will make clear which organizations are assured and which organizations are no longer assured of safe harbor benefits. An organization applying to participate in a self-regulatory body for the purposes of re-qualifying for the safe harbor must provide that body with full information about its prior participation in the safe harbor.

CONCLUSION

This safe harbor arrangement has been called a major accomplishment for both the U.S. and the EU. It comes at a time when trade disagreements rather than agreements between the U.S. and Europe dominate the news. The framework has also been labeled a landmark accord for electronic commerce. It bridges the different approaches of the US and the EU to privacy protection in a way that protects EU citizens' privacy when it is transferred the U.S., maintains data flows, and creates the necessary environment for electronic commerce. And it will provide predictability for U.S. companies. At the same time, the arrangement demonstrates EU recognition that a carefully constructed and well-implemented system of self-regulation, as advocated by the Clinton Administration, can protect privacy. It is a creative and innovative vehicle, perhaps the first international framework to rely on the private sector for its implementation. It thus can serve as a model in other contexts as we seek to ensure the development of seamless global environment for electronic transactions

The challenge in providing privacy protection in the Information Economy is to balance appropriately the free flow of information against the individual's right to privacy so we do not jeopardize the benefits these new information technologies promise or trench on the First Amendment. Whether the safe harbor will provide that balance remains to be seen. Sufficient numbers of companies will have to join the safe harbor and consumers will have to feel comfortable with how their personal information is used and their ability to control its use, if the safe harbor is ultimately to be judged a success.

EUROPEAN COMMISSION'S MODEL CONTRACTUAL CLAUSES: PAVING THE WAY FOR INTERNATIONAL TRANSFERS OR A NEW HURDLE?

by Barbara S. Wellbery and Rosa Barcelo [1]

INTRODUCTION

The European Union Data Protection Directive (the "Directive") and Member State laws that implement the Directive set out certain rules for ensuring privacy protection of personal information.[2] Article 25 of the Directive, which deals with international transfers of private data, specifies that personal information may be transferred to third countries only if the third country in question ensures an adequate level of privacy protection.[3] The Directive does not define what is meant by adequate privacy protection, although there appears to be consensus that the adequacy standard does not require privacy protection equivalent to that required by the Directive, but a lesser level of privacy protection.

The Directive provides for several different ways of satisfying its adequacy requirement. The European Commission ("Commission") may find that a third country

---

[1] Barbara Wellbery is a partner in the Washington, D.C. office of Morrison & Foerster and may be reached at <bwellbery@mofo.com>. Rosa Barcelo (Ph.D) is an associate in the Brussels office of Morrison & Foerster and may be reached at <rbarcelo@mofo.com>.

[2] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995, pp. 31-50.

[3] The Directive provides for several exceptions from this requirement. See footnote 6.

or sector ensures an adequate level of protection under Article 25 of the Directive.[4] This was the ground used by the Commission last July when it issued an adequacy determination with respect to the safe harbor framework negotiated by the United States Government and the European Commission.[5]

Companies in the United States that choose not to participate in, or are not eligible for the safe harbor,[6] but wish to receive personal information from the European Union ("EU") legally, must identify an applicable exception in the Directive[7] or use another means of establishing adequacy. Agreements entered into between European Union exporters of personal information and importers established elsewhere in the world are one legal basis contemplated by the Directive for establishing adequacy.[8] For many companies, they are the preferred alternatives where an adequacy determination by the European Commission is not available.[9] The Directive contemplates two different kinds of agreements—*ad hoc* or "one-off" agreements and standard or model clauses—that may ensure an adequate level of protection for data transfers.

The Commission has proposed draft model clauses,[10] and the Member States are in the process of considering those clauses and may approve them in the near future. This article provides a brief overview of the use of model clauses to satisfy the Directive's adequacy requirement and analyzes the requirements of the proposed model clauses. The article then reviews several concerns that industry groups and the U.S. Government have identified about the model clauses, as well as the EU procedure and timing for approving those model clauses.

ESTABLISHING ADEQUACY THROUGH CONTRACTS

EU exporters of private data and importers located elsewhere in the world may rely on *ad hoc* contracts to satisfy the Directive's adequacy requirement.[11] Under this approach, the agreements often incorporate by reference the data protection law of the Member State in which the data exporter is established. Because there are differences among the data protection laws of the 15 EU Member States, companies importing data from several Member States may find themselves having to comply with as many different privacy regimes as there are EU countries in which they do business.

In addition, the Member State authority in the country in which the data exporting company is located ultimately decides whether a particular agreement provides an adequate level of protection. The procedure for obtaining Member State approval varies among Member States, both in terms of the steps to be followed and the time frame. Generally speaking, however, most Member States require approval of ad hoc contracts by the data protection authorities in the Member State from which the data is being transferred.[12] Approval generally takes a minimum of one to two months, if no issues arise regarding the proper completion of the necessary forms or any aspects of the proposed data transfer.

The Directive also contemplates model contractual clauses as one means of providing adequate safeguards for the international transfer of personal information.[13] These clauses were expected to offer a simpler and more streamlined approach to

---

[4] Articles 25.6 and 31.2 of the Directive.

[5] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25 August 2000, pp. 7-47.

[6] In order to be eligible for the safe harbor, organizations must be subject to Section 5 of the Federal Trade Commission Act or must be air carriers subject to 49 U.S.C. 41712. Because telecommunications commission carriers and many financial services companies are not subject to the Federal Trade Commission Act, they are not eligible to join the safe harbor.

[7] Article 26.1 of the Directive provides several exceptions from the adequacy requirement. These permit the transfer to take place without an adequacy determination where the information is necessary to complete a contract between the company and the individual or the individual has given his unambiguous consent.

[8] Article 26.2 of the Directive.

[9] Relying on the Directive's exceptions can prove cumbersome and/or severally limit a company's use of personal information. For example, under German law for the consent to constitute a valid legal grounds for data transfer, such consent must be digitally signed. See also footnote 8.

[10] *See* Draft Commission Decision pursuant to Article 26 (4) of the Directive 95/46/EC on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries; <http://europa.eu.int/comm/internal—market/en/media/dataprot/news/clauses.html>.

[11] Article 26.2 of the Directive.

[12] The UK, Ireland and Sweden do not require approval of these contracts by the data protection authorities; all other Member States do.

[13] Article 26.4 of the Directive.

ensuring adequacy. Because the same set of clauses could be used for the entire EU and approval by Member State data protection authorities would not be required,[14] it was hoped that model clauses could facilitate transfers of personal data to third countries that are not subject to adequacy determinations. For example, if a multinational company with offices and employees in each Member State wanted to use model clauses as the legal ground to transfer personal information to the United States, it could use the same model clauses for all the data transfers from the 15 Member States. This would enable such companies to apply one privacy regime for all the information they receive from the EU.

REVIEW OF PROPOSED MODEL CONTRACTUAL CLAUSES

The proposed model contractual clauses ("model clauses") consist of ten clauses and several appendices. It is important to note that the model clauses provide a minimum threshold; the contractual parties may provide for additional conditions in their contracts if they wish to do so.

The model clauses include the following requirements:

- *Obligations of the Data Exporter.* The clauses require that the data exporter comply with the requirements of the relevant data protection law in the country where it is located up to the time of the transfer,[15] to inform the data subjects "at least at the moment of the transfer" that their data could be transferred to a third country,[16] to make available upon request copies of the clauses to individuals whose data is transferred, and to respond to inquiries from such individuals and the data protection authority.[17] Several requirements imposed on the data exporter appear to go beyond the requirements of the Directive and/or national legislation, such as the obligation to provide copies of the clauses to individuals whose data is transferred.
- *Obligations of the Data Importer.* The parties may decide either that the data importer will comply with the privacy laws of the country in which the data controller is established or with the relevant provisions of any Commission adequacy decision, as long as the data importer is based in the specific third country to which the decision applies and is not covered by the adequacy decision.[18] The parties may also elect to comply with the Mandatory Data Protection Principles, which are annexed to the model clauses as the "Annex to the Contract. If the parties choose either the country in which the data controller is established or the relevant provisions of any Commission adequacy decision, however, the data importer also must agree to comply with certain principles embodied in the Mandatory Data Protection Principles. In particular, the data importers must comply with the purpose limitation requirement, restrictions on onward transfers, and rights of access, rectification, deletion, and objection. These Mandatory Data Protection Principles require, among other things, that personal data be processed only for the *specific purpose* for which they were transferred and not for any other purpose,[19] that the data be transferred to a third party (established outside the EU) only where the importer has either obtained the informed consent (opt in for sensitive data, opt out for non-sensitive information) of the individual or the third party becomes a party to the contract between the data exporter and importer,[20] and that the importer give individuals right of access to their data, rights of rectification, and deletion and objection.[21]

These three Mandatory Data Protection Principles, purpose limitation, access, and onward transfer, appear to require more than the safe harbor principles require. For example, the safe harbor rules allow the importer to use the data for different purposes from which they were initially transferred, unless such purposes are incompatible with the purpose for which the data were originally transferred. And, the safe harbor access principle is subject to a proportionality or reasonableness standard.[22] Accordingly, data importers relying on model clauses would be subject to greater restrictions on their use and transfer of data than those data importers relying on the safe harbor adequacy decision. It would appear that the model clauses also go beyond other laws, which the Commission is about to consider as affording

[14] Article 26.4 of the Directive
[15] Model Clauses, Clause 4(a).
[16] Model Clauses, Clause 4(b).
[17] Model Clauses, Clause 4(c).
[18] Clause 5(c) of the Model Clauses.
[19] Annex to the Contract, par. 1.
[20] Annex to the Contract, par. 6.
[21] Annex to the Contract, par. 5.
[22] *See* Safe Harbor Privacy Principles (2000), available at <www.export.gov/safeharbor>.

an adequate level of protection,[23] and may even be more restrictive than the Directive.[24]

In addition, data importers must agree to submit to audits of their data processing facilities at the request of the data exporter and to cooperate with data protection authorities in inquiries and abide by their advice. Investigations may be carried out by the exporter itself or by a body selected by the exporter "in agreement with the Supervisory Authority" and composed of independent members with required qualifications.[25] The data importer also must warrant that it is not subject to national legislation that restricts compliance with the data protection principles beyond that which is contemplated in Article 13 of the Directive.[26] It also is not clear that U.S. companies will be able to provide this warranty. Article 13 lists several grounds, such as national security, defense, public security, and protection of rights and freedoms of others, but does not specifically list free speech rights, which in the U.S. may limit compliance with data protection principles.[27] It is not clear at this time if the EU will view Article 13 as encompassing the free speech rights guaranteed by the First Amendment to the U.S. Constitution.

Liability

Model Clause 6 establishes that importers and exporters will be jointly and severally liable for breach of the conditions and obligations imposed by the agreement. The Commission justifies the use of the joint liability standard in light of the fact that it can be very difficult for consumers to know who the responsible person is and how to enforce the clauses against an importer located in another country. Accordingly, Clause 6 allows importers to be exempt from liability if they can prove that the data exporter is solely responsible for any damage. Parties are free to agree on mutual indemnification.

Applicable Law and Enforceability of the Clauses

Individuals whose data are transferred to a third country under the model clauses have the rights of third party beneficiaries and may enforce the privacy provisions of the contract against any of the parties.[28] The applicable law for determining damages will be the law of the country where the individual resides.

Jurisdiction

The parties to the model contract must agree that if a dispute arises that is not solved amicably, the data importer will accept the courts of the Member State in which the aggrieved individual resides, third party mediation, the data protection authorities where the data exporter is located, and arbitration. The aggrieved individual has the right to decide which of these to use to pursue his or her claim and may elect to pursue his or her claim in more than one forum at the same time.[29]

CONCERNS ABOUT THE PROPOSED MODEL CLAUSES

Several different entities have expressed concerns with the model clauses. These fall into two broad categories: substantive concerns and procedural concerns. Any discussion of concerns about the Commission's model clauses must begin with two basic points:

First, the Directive by its very terms restricts crossborder data transfers, although these are essential for international business. Therefore, it is crucial that the Commission identify mechanisms that provide adequate privacy protection without imposing unnecessary significant burdens and costs on data exporters and importers. If it does not, the Directive ultimately either will damage the ability of EU companies to engage in trade and realize the potential of electronic commerce, and/or discourage the very compliance that the EU seeks to engender.

---

[23] For example, the Commission is expected to find the new Canadian law adequate, although Canadian law does not incorporate an explicit provision limiting onward transfers.

[24] Indeed, according to Article 6 b of the Directive, data controllers are entitled to use the collected data for purposes other than those for which the data were initially collected, provided that such secondary uses are not *incompatible* with the use for which the data were initially collected. The Commission has not clarified why the same principle can not be used in the context of the Model Clauses.

[25] Model Clauses, Clause 5.

[26] Model Clauses, Clause 5(a).

[27] *U.S. West, Inc. v. FCC,* 182 F.3d 1224 (10th Cir. 1999), *cert. denied,* 2000 U.S. LEXIS 3811 (2000).

[28] Kotschy, W., Model contracts for transborder flows: A way forward, International Newsletter, Issue no. 56, December 2000, pp. 4-10. The third party beneficiary clause will put the individual in a position to enforce all or certain of the contractual obligations, which to some extent is comparable with the rights that the individual has according to his/her domestic law.

[29] Model Clauses, Clause 7.

Second, as noted above, the model contract clauses are intended for use between data exporters located in the EU transferring data to data importers that are not covered by a Commission adequacy determination. Since the Commission has issued only three adequacy determinations thus far[30] and is unlikely to issue decisions for more than a limited number of countries in the medium term, model contract clauses will be the only truly viable option for data transfers from the EU for most of the world.[31] For these reasons, at least, it is essential that the model clauses provide a reasonable basis for personal data transfers from the EU to other countries.

Substantive Concerns

The major substantive concerns that have been raised with the model clauses turn on their lack of usefulness for international data transfers. For example, the Confederation of British Industry ("CBI") has noted eight general reservations about the standard clauses (in addition to a long list of specific concerns). These concerns can be summarized by the conclusion that the clauses cannot be used commercially since they are unnecessarily burdensome and prescriptive. CBI also is of the view that the model clauses impose too heavy a burden on the data importer and, in some cases, impose requirements that exceed those of the Directive.

The International Chamber of Commerce ("ICC") also has identified a long list of concerns about the model clauses. These include the imposition of joint and several liability and jurisdictional submission by the data importer. In the ICC's view, joint and several liability is inappropriate in the data protection situation where responsibility for a breach can be identified. In addition, joint and several liability will discourage use of model clauses and/or reduce the certainty such clauses could otherwise provide, as parties would have to negotiate indemnification clauses individually. The ICC also takes the view that jurisdictional submission should be a matter of last resort, to be required only where absolutely necessary.

The United States Departments of Commerce and Treasury also have identified several substantive concerns with the model clauses (while noting that their list is not exhaustive). In a letter to the European Commission, they indicated that model clauses might create several adverse consequences for U.S. enterprises. The Commerce and Treasury Departments stated that the model clauses could undermine last year's agreement to permit use of the safe harbor principles for the substantive privacy provisions in model contracts. Their letter also noted that the model clauses appear to impose burdensome requirements that exceed what was agreed by the Department of Commerce and the European Commission.[32]

In addition, and perhaps most basically, a major problem with the model clauses is that they require more than adequacy. Instead, the model clauses require privacy protection equivalent to that required by the Directive. Companies either have to comply with Member State laws or they have to "top up" beyond the adequacy decisions the European Commission has rendered. Also, the model clauses obviously and inexplicably disadvantage U.S. financial services companies and telecommunications companies. These companies are unable to take advantage of the safe harbor or other adequacy decisions. (*See* footnote 7.) And, assuming that the European Commission as expected issues an adequacy determination with respect to the new Canadian privacy law, the model clauses also would disadvantage those Canadian companies not covered by the new privacy law. Those companies that do (or will) not fit within those adequacy determinations either will have to rely on other limited exceptions to the Directive, *ad hoc* contracts with their time-consuming approval requirements, or more restrictive and burdensome model contracts.

The proposed model clauses also fail to allow for one of the major anticipated benefits of model clauses: one privacy regime for all personal information being imported from the EU, regardless of where in the world a company's offices are located. Instead, companies will have to adhere to a number of different privacy regimes when they import personal data from the EU. A U.S. company importing personal data from EU countries will be faced with a patchwork of privacy requirements. Personal information imported by a U.S. company from France to the U.S., for example, may be handled in accordance with the safe harbor. If that same company imports data from France but to Japan, it will have to be handled in accordance with French privacy law. And if the company imports personal information

---

[30] Only Switzerland, Hungary and the companies that abide by the safe harbor are considered as providing an adequate level of protection for personal data transferred from the EU. The Commission has initiated a procedure to assess whether Canadian law provides an adequate level of protection, and it appears that it will conclude that it does provide such protection.

[31] Model Clauses, recital 5.

[32] The Department of Commerce has also sent to the European Commission far more extensive comments on the model clauses. See DOC Staff Comments on the Model Contract Provisions, January 16, 2001.

from other EU countries to Japan, it will have to adhere to the privacy laws of each of those countries while the personal data is handled in Japan. Yet companies increasingly are global and information is now routinely shared on firm Intranets and/or centralized in data bases in one location with access possible from a company's offices around the world. It is difficult to see how this patchwork of requirements can be effective, or will be enforced. And, the EU has provided no indication of why such a cumbersome approach is necessary or justified to provide the adequate privacy protection required by the Directive.

Procedural Concerns

Serious concerns also have been raised about the transparency of the process used by the Commission in adopting these clauses. The European Commission has been working on draft model clauses for the transfer of personal data to third countries since mid-2000. The first version was posted on the Commission's web site for public consultation in September 2000. From October through mid-January, the Commission redrafted the draft clauses several times in light of comments and suggestions made by representatives of Member States, the Working Party 29 on the Protection of Individuals,[33] and interested parties such as business and consumer associations. The latest draft was completed on January 19, 2001. Although the draft had changed dramatically in the interim, it was not made available to the public until February 15, 2001, two working days before the Article 31 Committee's vote on the model clauses was scheduled to take place.[34] Accordingly, the ICC, for example, has taken strong objection to the lack of transparency in the Commission's process and has urged the Commission to initiate an open and broad process of consultation.

NEXT STEPS

On February 19-20, 2001, the draft model clauses were submitted for approval to the Article 31 Committee, a group of Member States representatives. To everyone's surprise, the Article 31 Committee did not approve the draft clauses. Officially, the result has been attributed to the fact that some Member States felt they needed more time to give proper consideration to the content of the draft clauses. Unofficially, however, several Member State officials have acknowledged concern about the process and its lack of transparency, as well as with the substance of the clauses. The Article 31 Committee meets again at the end of March 2001. If the Article 31 Committee approves the draft clauses, the European Parliament will have one month to assess whether the European Commission has exceeded its power in approving them. The Parliament is not competent, however, to give an opinion on whether the standard contractual clauses ensure an adequate level of protection or not, although the Parliament may do so in any event as they did with respect to the safe harbor. Upon completion of this procedure, the Commission will adopt the decision and publish it in the Official Journal. If approved at the March meeting of the Article 31 Committee, the model clauses are expected to be operational by September 2001.

CONCLUSION

The European Commission and Member States have found that the safe harbor and certain national laws provide adequate privacy protection. These entities also are expected to issue an adequacy decision on the new Canadian privacy law shortly. One would expect that those same self-regulatory and legislative frameworks also would provide adequate privacy protection when embodied in model clauses. Yet the model clauses as proposed by the Commission would require a higher level of privacy protection than is required by those adequacy decisions. Some have claimed that they require privacy protection equivalent to that required by the Directive. In some instances, the model clause requirements seem to require even more than the Directive. Yet the Commission has not explained why it would impose more restrictive requirements upon those who use model clauses as legal

[33] The Article 29 Committee is a committee composed of representatives of the European Commission and the Member States and is responsible, inter alia, for issuing opinions on the meaning of the Directive. These opinions are designed to lead to a harmonized application of the Directive throughout the EU. The opinion on the standard model clauses is: Opinion 1/2001 on the Draft Decision on Standard Contractual Clauses for the transfer of Personal data to third countries under Article 26(4) of Directive 95/46, Adopted on 26th January 2001, <http://europa.eu.int/comm/internal—market/en/media/dataprot/wpdocs/wp38en.html>.

[34] The Article 31 Committee is a committee composed of representatives of Member States, usually officials of the Ministry of Justice, as well as a representative of the Commission. This Committee is competent to deliver opinions as to whether the legal regime of a non-EU country ensures an adequate level of protection.

grounds for data transfers or why it believes it is permissible to go beyond the adequacy decisions it has already rendered.

Indeed, during the safe harbor negotiations, many of the Member State data protection authorities repeatedly indicated a clear preference for model contracts and tried to turn the discussion from the self-regulatory model embodied in the safe harbor to model clauses. These authorities argued that the model clauses would provide greater privacy protection since they did not rely on self regulation. Therefore, it is particularly difficult to reconcile the approach on model clauses being taken by the European Commission. The effect (whether intentional or not) will be to penalize companies that rely on them and to dissuade companies from using them.

Mr. STEARNS. Ms. Waggoner?

STATEMENT OF DEBRA L. WAGGONER

Ms. WAGGONER. Thank you.

Mr. STEARNS. Welcome.

Ms. WAGGONER. Chairman Stearns, Mr. Towns, thank you very much for the opportunity to testify this afternoon. I am here today on behalf of the Information Technology Industry Council, ITI, and it represents members who are in the information technology and leading the world in global e-commerce.

Mr. Vradenburg's testimony parallels much of what ITI is about. They are a member in good standing, so we endorse much of what his statement is. So I will be brief today, rather than make you listen to the same key points.

Today there are 300 million people on the Internet, and by 2005, there will be over a billion people on the Internet. With this global connectivity, digital trade is naturally becoming a more important part of the global GDP. Chairman Stearns mentioned that by 2004 b-to-b commerce and b-to-c commerce will reach $7 trillion.

All of this will be important. It is important in a number of sectors, both in software, in online music, and we hope online video. But that assumes that there will be sufficient broadband deployment to accommodate this growth in e-commerce.

Developed and developing nations are particularly aware that telecommunications is the foundation of the Internet, and the Internet is the foundation of e-commerce. As nations take steps to make their telecom environment hospitable to spur Internet and e-commerce growth, businesses and policymakers face a significant challenge. Businesses must navigate myriad national regulatory, technical, and operational environments, while policymakers must build global consensus to encourage digital trade.

Because the communications infrastructure is so important to the Internet and e-commerce, efforts must be continued globally to ensure telecommunications regulatory reform that enhances competition and encourages broadband deployment so that e-commerce can grow and flourish. Telecommunications reform is particularly important in developing nations where many countries are still in the process of privatization global government monopolies. Further liberalization of trade and services is particularly important to provide the infrastructure, to support e-commerce, and to engage electronic delivery of services. A great deal of potential e-business activity will be found in the services sector, including finance, telecommunications, logistics management, and education, which are creating the reality of a global infrastructure.

Finally, let me underscore a point raised earlier. We must establish a strong foundation for digital trade by first confirming that

WTO obligations, rules, and disciplines apply to e-commerce, especially the General Agreement on Tariff and Trades, the General Agreement on Trade and Services, and strong protection of intellectual property for goods and services in accordance with the WTO TRIPS Agreement.

In closing, ITI applauds you, Mr. Chairman and members of the committee, the State Department, and the Office of the United States Trade Representative for recognizing the importance of digital trade and the necessity of addressing it in trade negotiations. As the U.S. moves ahead with bilateral, regional or a new WTO round of trade negotiations, we recommend the guiding principles outlined by ITI to provide a foundation for moving forward. Thank you.

[The prepared statement of Debra L. Waggoner follows:]

PREPARED STATEMENT OF DEBRA L. WAGGONER, DIRECTOR, PUBLIC POLICY, CORNING INCORPORATED ON BEHALF OF THE INFORMATION TECHNOLOGY INDUSTRY COUNCIL

Thank you Mr. Chairman for inviting me to testify today on the issue of Digital Trade. I am here today on behalf of the Information Technology Industry Council (ITI), which represents the leading providers of information technology products and services (a membership list is attached). We advocate expanding economic growth through innovation and support free-market policies. Our industry is truly global, with more than 50% of member company revenues derived from foreign sales. Our members had worldwide revenue of more than $633 billion in 1999 and employ more than 1.3 million people in the United States. I chair ITI's International Committee, which has been engaged in global e-commerce issues now for a number of years.

My message to you today is simple: e-commerce and digital trade are reshaping the global economy; digital trade benefits all countries; and we need to advance an agenda for Digital Trade Policy that promotes growth, wealth creation and societal benefit. I want to provide you with the broader context of the global networked economy and lay out an agenda for digital trade policy. Owing to the global nature of our industry, we want to pursue this digital trade agenda through all available trade agreements "whether bilateral, regional or multilateral.

Trade Liberalization in a Networked Global Economy

Three powerful and related trends are fundamentally reshaping the global economy: 1) the exponential growth in Internet connectivity, 2) the convergence of content, interactivity, computer applications and communications networks, and 3) the increasing use of electronic commerce as a channel for conducting international business. Today, more than 300 million people around the world are online; by 2005, one billion people will be connected to the Internet, more than 75 percent of them outside North America. This technological transformation is creating a networked global economy that is just beginning to demonstrate that e-commerce and the Internet can be powerful engines for economic growth.

Recent economic data bear this out. Digital trade is becoming a more important part of global GDP. For example, between 1999 and 2003 the market for electronically distributed software is projected to grow from $500 million to approximately $15 billion. Online music revenues are expected to grow from $850 million today to $4.3 billion by 2004. The growth of online videos is expected to grow exponentially as well if there is sufficient rollout of broadband communications platforms. And business-to-business e-commerce is expected to grow from $403 billion in 2003 to over $7 trillion in 2004.

Digital trade presents a new opportunity to advance the goal of expanded international trade in a converging, networked environment. The Internet and electronic commerce can greatly facilitate trade, providing a new means for conducting global commerce and delivering digital goods and services to all parts of the world. Trade negotiators must now ensure that new technologies, new business models, and new products are available to consumers, businesses, and governments around the world so these users can benefit from increased productivity, competition, and choice. Existing trade agreements provide a good foundation for this work but need to be expanded to address these new realities. Trade negotiators must also protect against the creation of new trade barriers in a sector that has flourished with little or no regulation.

Digital Trade

Digital trade encompasses cross-border e-commerce transactions, global e-business relationships, and the specific goods, services, and intellectual property protections that act as enablers for these transactions and relationships. A successful digital trade policy must address all of these areas. Digital trade includes:

E-Commerce Transactions

- Goods and services that can be ordered and delivered electronically.
- Goods and services that can be ordered electronically but are delivered physically.

E-Business Relationships

- Integrated international supply chains facilitated by global networks.
- Outsourcing arrangements that utilize global networks.
- Business partnerships, joint ventures, and "virtual corporations" enabled by these networks.

E-Commerce Enablers

- Goods—Information technology (including computer hardware, software, and communications equipment) is critical to building and expanding the networks over which all digital trade is conducted, so free trade in IT products is essential to promoting digital trade.
- Services—Many services are needed to enable an e-commerce transaction, including telecommunication services, computer and related services, financial services, advertising services, distribution services, and express delivery services. Collectively, these services are often referred to as the "e-commerce value chain." Liberalization across this value chain is essential for ensuring seamless, cost effective and timely business-to-business and business-to-consumer transactions.
- Intellectual Property—If individuals and companies are to provide their digital goods and services over the Internet, then they must be assured that their intellectual property will be protected in this new online environment.

Digital Trade Benefits All Countries

In the United States, the new economy has had a significant impact on overall U.S. GDP and the U.S. balance of trade. Nearly two-thirds of productivity gains can be traced to high-tech investments made over the past five years. Specifically, information technology contributed over one-third of economic growth since 1995, and IT exports amounted to more than one-quarter of total U.S. exports in 1999.

Already there is evidence that the development of emerging economies is being reshaped and energized by online trade. The traditional model of infrastructure investment and international trade is being complemented by electronic commerce. This is leading to a dramatic expansion of opportunities for economic development, driven by businesses creating new markets for innovative products and services being made available electronically throughout the world. In particular, evidence shows that businesses in every region of the world can, by means of electronic commerce, dramatically reduce costs of entry, maximize efficiency, and vastly expand distribution to previously inaccessible markets.

An Agenda for Digital Trade Policy

To promote the growth of digital trade and to ensure that electronic commerce benefits from trade liberalization, ITI proposes the following digital trade agenda. This agenda should be pursued through all available trade agreements, whether bilateral, regional, or multilateral.

Guiding Principles for Digital Trade

- Current WTO obligations, rules, disciplines and commitments, namely the GATT, GATS and TRIPS agreements, should apply to e-commerce.
- Electronically delivered goods and services should receive no less favorable treatment under trade rules and commitments than like products delivered in physical form, and their classification should ensure the most liberal treatment possible.
- Governments should refrain from enacting trade-related measures that impede e-commerce.
- When legitimate policy objectives require domestic regulations that affect e-commerce, ensure that such regulations are transparent, nondiscriminatory, and employ the least-trade-restrictive means available.

Information Technology Tariffs and Non-Tariff Measures

Tariffs and non-tariff measures applied to information technology products should be eliminated or phased out. Tariff and non-tariff measures act as a counter-productive tax or burden that raises the cost of the very technology needed to be competitive in the digital economy.

Countries that have not done so should sign and immediately implement the Information Technology Agreement (ITA). In the context of the ITA, governments and business must continually update the definition of what constitutes an "IT product" to keep pace with technological developments. Non-tariff measures, in particular redundant testing and certification procedures, should be eliminated where they exist.

Services Commitments

Trade in services negotiations, whether in the WTO or other venues, offer an excellent opportunity to promote digital trade. Increased liberalization of trade in services will play an important role in the promotion of digital trade in several ways:

E-Commerce Value Chain: Improved market access and national treatment commitments in the group of services sectors that are necessary to initiate and complete an e-commerce transaction will expand digital trade opportunities. Two particular elements of the value chain deserve special mention:

- *Telecommunication Services:* Telecommunication services provide the network infrastructure that is a fundamental prerequisite for digital trade. Competition in the provision of these services is critical to the growth of digital trade. Full basic telecommunications commitments, including implementation of the pro-competitive Reference Paper principles, as well as full value-added services commitments and protections against anti-competitive behavior by incumbent telecommunications companies in the value added services market are important objectives. On the other hand, competitive value-added services, including Internet services, should not be subjected to regulation created for monopoly basic telecommunications markets.
- *Evolving IT Services:* The Internet provides a new means for delivering information technology services; and technologies and business models are evolving much too rapidly for trade classification discussions to keep pace. Trade negotiators should seek ways to ensure that broadly defined or interpreted market access commitments will enable cross-border trade in evolving IT services. It is also important that unregulated IT services not be viewed as a subset of regulated telecommunication services.

Electronically Delivered Services: In addition to liberalizing services that enable e-commerce transactions, trade negotiators should seek improved market access and national treatment commitments for a broad range of services that can be delivered electronically.

Intellectual Property Protection and Market Access

Intellectual property rights in goods and services traded on the Internet should be afforded strong protection in accordance with the WTO TRIPS Agreement and the WIPO Treaties. Without such protection, content creators, service providers and users will be less likely to realize the tremendous benefits of digital trade.

Greater market access for digitized software, music and videos will go a long way toward helping to reduce piracy rates. Without market access for legitimate products, our companies face difficult hurdles in protecting their intellectual property. Market access for digitized products will also be an important first step in promoting trade and cultural diversity, since today's successful business models have been ones that tailor the global reach of the Internet to local interests and tastes.

Allowing U.S. Companies, Workers and Consumers to Continue to Lead & Prosper

In closing, ITI is pleased that Members of Congress and the Office of the U.S. Trade Representative recognize that digital trade is an increasingly important component of international trade and are actively addressing these issues in trade negotiations. We believe that trade rules designed to ensure access to e-commerce markets will allow American companies, workers and consumers to continue to lead and prosper in the networked global economy. As our own market matures, the U.S. IT industry is looking toward new markets, particularly those in Latin America and developing countries in Africa and Southeast Asia. While many of these countries realize the benefits that can accrue from investment in IT infrastructure, they are hampered by domestic policies that maintain high tariffs on IT products or by regulatory policies. As the U.S. moves ahead with bilateral, multilateral or a new Round of WTO trade negotiations, we would urge that the guiding principles outlined above be a foundation for going forward.

Thank you, Mr. Chairman, and I would be happy to answer any questions you might have.

Mr. STEARNS. Let me open with the questions here. Ms. Wellbery, you are probably, from the private sector, the expert here on the Hague Convention, and we had, I think his name is Dr. Rodata—Stefeno Rodata, who was the Chair that developed the Internet privacy standards for the European community. And he came here and testified, and then when I asked him, I said, "Well how many people in America—what major large corporations have signed up under the Safe Harbors that the Clinton Administration had negotiated," he said 30. Well, obviously, that is not a lot. And so my question to you, you seem to indicate it is working, but we found only 30 large corporations have signed up for the Safe Harbors. What is the problem? Why haven't more signed up? Because then the Doctor went on to say he is developing model contracts now to try and bridge this gap and get individual companies to sign up.

Ms. WELLBERY. I think since the hearing that you are referring to, the number has gone up to somewhere over 40 companies that have signed up. But I agree that that is not a lot of companies, and I think there is a number of reasons that explains why that is the case.

First, I think it takes a long time to get companies' privacy policies and practices in line with the requirements of any privacy regime. We certainly know from our own domestic experience with Gramm-Leach-Bliley that it has taken companies a long time to come into compliance with that act. And a similar kind of analysis of companies' practices and policies needs to be done to come into compliance with the Safe Harbor requirements.

I think a number of companies were also waiting to see what the European Union was going to do about model contracts and whether those would be a more appealing or attractive alternative. I think the decision that was issued by the commission makes clear that they are far more onerous than the Safe Harbor, and so they are likely to be a far less attractive option for U.S. companies.

In addition, I think that there are some companies that are just doing the analysis wrong. They wonder why they would subject themselves to liability before the FTC, but they ignore the fact that by transferring information from Europe without a legal basis, they are exposed to liability or at least their European affiliated companies are exposed to liability in Europe.

And then, finally, I think we have a little bit of "Alphonse and Gaston" here. Everybody is waiting for the other company to go first, and I wonder if the fact that Microsoft has now announced that it will be joining the Safe Harbor will lead to a larger number of companies joining the Safe Harbor. Thank you.

Mr. STEARNS. Well, it is nice to have you here, because you were chief negotiator. I mean you have been involved with it. You know it more intimately than anybody, so we are always puzzled why this thing hasn't take off. And the European Union does not intend to enforce their policy for a while. Did they ever tell you—do you have any indication when they are going to start enforcing their policy?

Ms. WELLBERY. Well, I think they are enforcing their laws now. My law firm actually does monitor enforcement actions in Europe.

Mr. STEARNS. Okay.

Ms. WELLBERY. Most of them have been against—in fact, almost all but one have been against European companies. I am only aware of one enforcement action that has been brought against a U.S. company.

Mr. STEARNS. Okay. Mr. Kovar, you have heard some of the, not necessarily criticisms, but her comments in her opening statement during this process. You might want to reply to any portions that she had said about the Hague Convention.

Mr. KOVAR. Thank you, Mr. Chairman. I think, as I indicated in my statement, it is an extremely complex convention, and it is made even more difficult by the need to fit the relatively unknown quantity of Internet transactions into the jurisdictional framework. And I don't have any answers on the best way to do that. We are still listening.

I think, to respond to one point that I think was one of the principal thrusts of Ms. Wellbery's statement, which is the notion that perhaps somehow this convention would open up U.S. courts in a new way to enforce judgments coming from abroad, that is one area where we are not quite sure that that would be the case. Right now, U.S. courts are basically wide open to enforcing foreign judgments. And the enforcement section of this treaty mirrors in many ways current U.S. law in all the States. And for that reason, that is one concern that to us doesn't seem to have as much weight behind it as some of the other questions about what the jurisdictional rules should be.

Mr. STEARNS. This is still a question that puzzled me in the hearing we had with the European Union. So a company like Microsoft signs up for the Safe Harbor. Does that mean that when you develop model contracts, they will retroactively be applied to or how do the model contracts in the Safe Harbor—how does that work for companies?

Ms. WELLBERY. There are a number of different options that companies can use for exporting or, I guess a better to say it is, for importing data from the EU to the U.S. There are exceptions that are created in the EU directive. You can use individual or one-off contracts, you can use model contracts, you can use consent of the consumer, and you can use the Safe Harbor. These are all alternatives.

And in negotiating the Safe Harbor, what we were trying to do was to provide another alternative for U.S. companies that hopefully would be a more streamlined, more efficient, and more effective way of transferring data out of Europe to the U.S.

For example, when you use contracts—when you use one-off contracts in Europe, I think it is 13 of the members—15 member states require prior approval of those contracts. And these prior approvals can take 1 to 2 months to obtain assuming that you have all the information in the right places in the first instance. If you don't have all that information correctly there, it can take much longer. And the Safe Harbor does away with those bureaucratic requirements.

Mr. STEARNS. Ms. Waggoner, just briefly, just give us the most significant trade barriers to digital delivery of goods, in your opinion.

Ms. WAGGONER. I think that for the IT industry, the most difficult barrier is that of wrong action. Forbearance is probably more important in this area. Right now we face few barriers. I think intellectual property protection, making sure that we have strong IP is probably a very important one. Expanding coverage of the services agreements would be another. But, again, I think we would urge forbearance, because it is the danger of action in the wrong direction in this burgeoning field that probably stands to harm us more than current action.

Mr. STEARNS. Do no harm. My time is expired. Mr. Towns?

Mr. TOWNS. Thank you very much, Mr. Chairman. Let me just start out by—Mr. Vradenburg, will AOL and Time Warner be signing onto the Safe Harbor Agreement?

Mr. VRADENBURG. We are looking at that——

Mr. TOWNS. Microsoft is on board.

Mr. VRADENBURG. Excuse me.

Mr. TOWNS. Microsoft is on board.

Mr. VRADENBURG. Well, we don't follow Microsoft in everything, Mr. Towns.

We are looking at that issue right now. In fact, we believe that we are substantially, if not totally, in compliance with existing EU Data Protection Directive provisions in Europe already. But there still are some useful things in taking advantage of the Safe Harbor rules, and so we are looking at that question right now. So I would suggest that some of this is a matter of time. I think that there is an indication that perhaps by July 1 a number of companies may well make a decision on whether or not to take advantage of the Safe Harbor guidelines or not.

Mr. TOWNS. Right. Thank you very much. Ms. Wellbery, sort of following up, I guess, on the Chairman's question, the fact that only 30 corporations have signed up, and you say, "Well, it takes a while." Why does it take so long?

Ms. WELLBERY. Because I think when you work with companies, they have been collecting information in many disparate ways, and it is being stored in many disparate locations, and one of the things you have to do when you start to develop a privacy policy is to figure out all the ways in which you are collecting information, where you are storing it, how you are using it, and whether you are providing the required opportunities for customers to opt out before you can put a policy in place. And that can be, for a large organization, extremely time-consuming. And then you also have to train your employees so that they, in fact, are implementing the policy that you say you have adopted. Once you say you have adopted the policy, if you don't, then you are subject to liability. So all of those things together can take quite a long time.

Mr. TOWNS. Thank you. Mr. Vradenburg, again, if common sense says that unmetered pricing for Internet access promotes greater Internet adoption and use, what is the problem internationally?

Mr. VRADENBURG. The problem here, Mr. Towns, is that in many countries of the world, the national, usually government-owned, telecommunications carrier charges by the minute for local tele-

phone calls. That is a system that they have built over time that favors the national telecommunications carrier. When the Internet has come along and now independent Internet services are carried over the local phone company, say, for example, in Germany, the local phone company makes some amount of money for every minute that someone's online on AOL. So if favors the national telephone carrier to be able to continue metered pricing even though it may not be in the interest of the adoption and the use of the Internet overall.

In Europe, the UK has a longstanding, independent regulatory authority OFTEL, which is now moved to require British Telecom to move toward flat-rate pricing. And as a consequence, Internet adoption has quickly kicked up in the UK. On the other hand, Germany has not adopted that policy. Deutsche Telecom has refused to proceed with it. And as a consequence, Internet adoption and use has slowed in Germany as compared to other countries. That is a policy that favors Deutsche Telecom, and the German government, of course, owns a major stake in German telephone system, so that you are not seeing an independent regulatory authority emerge in Germany to require flat-rate pricing, as you have seen in the UK.

Now, in the United States we have made a decision sometime ago, almost by accident at the FCC, that there would be no long distance charges for enhanced services. So the reason that you see flat-rate pricing in this country is that Internet calls have been treated essentially as local calls and not Internet calls. But every year you will see the phone companies coming back to that issue with the FCC in this country seeking to reclassify Internet calls into interstate calls and long distance calls so that they can meter the cost of Internet service in this country. But so far the FCC, in looking at this issue periodically, over a number of years, has stuck to its policy of assuring that Internet prices in the United States are on a flat-rate basis.

Mr. TOWNS. All right. Thank you. Thank you very much. Mr. Kovar, Ms. Richardson stated that the draft convention appears to do more harm than good with respect to protecting intellectual property, because it reflects that the discussion pre-dates e-commerce. What is or what will the State Department do to correct this and protect America's intellectual property, which is over 4.9 percent of the gross national product?

Mr. KOVAR. Thank you, Mr. Towns.

Mr. TOWNS. And I am going to ask Ms. Richardson to respond when you are finished here.

Mr. KOVAR. Oh, okay. Sure.

Mr. TOWNS. Go ahead.

Mr. KOVAR. Sure. The current draft of the convention, which dates back to 1999, has in it a provision that deals with patents and trademarks that is pulled right out of the European Convention of Enforcement of Judgments, called the Brussels Convention. No one likes it in this country. It wouldn't work well. And we have said that it is one of the major problems with that text.

We don't know exactly yet what the right formulation is to provide full protection for patented trademark interests. So what we have been trying to do is to get patent and trademark experts from

all sides to help us understand what makes the most sense. And in the same way in copyrights, which are actually treated in a different section of the convention, in a tort section. We have been grappling with exactly what is the best legal system of jurisdiction to deal at the international level with copyright protection. We don't have an answer to that yet, but we are trying to pull in as many of the interest groups as we can to help us find the right answers. Thank you.

Mr. TOWNS. Mr. Chairman, I know my time has expired, but I called Ms. Richardson's name.

Mr. STEARNS. We are going to have a second round here.

Mr. TOWNS. Okay. All right. Well, I am going to let her respond to it.

Mr. STEARNS. Yes, sure.

Ms. RICHARDSON. I just wanted to briefly make clear that we don't believe that the State Department is the enemy here. We very much appreciated his remarks today where he said this deserves careful consideration. If there is an enemy, it is just momentum. This negotiation has been going on a long time. A lot of the other countries out there think it is time to conclude it, and the e-commerce issues and new issues, they do deserve a lot of time and attention to sort them out. So as long as we get that, we will be, I think, happy.

Mr. TOWNS. I thought I was going to start a fight.

Mr. STEARNS. Thank you. The gentleman from Illinois.

Mr. SHIMKUS. Thank you, Mr. Chairman. And I was really focused—I was going to focus on the net metering too. We had a similar issue a couple years ago when the whole Internet service began, and it was the local call versus, in rural areas, the long distance call. The long distance calls were metered out where the local calls were not. And for those who tried to run businesses, when we talked about the ability to stay at home and work, we couldn't do that at the time, because we hadn't evolved to the issue of—we hadn't moved away from the net metering and local call issue. Now I think we have done that in this country, so I can understand that it is an issue and that it will be an issue I will take up with my colleagues when I go over there next week.

I want to briefly ask a response on the cultural content restrictions. And really, in my notes, I would like, of course, Ms. Richardson to respond to that. But also Mr. Vradenburg, Mr. Kovar, if you can address, and then anybody else who wants to throw in, and I think that will probably be enough of my time. Talk to me about the cultural content restrictions.

Ms. RICHARDSON. I am happy to kick that one off. Historically——

Mr. SHIMKUS. Pull that mike close to your mouth. There you go.

Ms. RICHARDSON. Really since the trade system began in the last forties, countries have been concerned about promoting their culture, and there is nothing wrong with that. We are as culturally diverse country as any on Earth, and we are proud of cultural diversity. One of the things about e-commerce is that it enhances cultural diversity. It solves the shelf space problem and allows producers and creators to reach out to wide audiences in a way that was never possible before.

Given that set of opportunities, it would be particularly a shame, troublesome, a crime if countries were to impose the kinds of cultural protectionism that they imposed in the Old World on top of the e-commerce world. We haven't seen it yet, and the best to get trade commitments to keep open markets open is before cultural protectionism has set in. So that is our goal.

Mr. VRADENBURG. Mr. Shimkus, this may be another agenda item when you visit Europe, because they are now embarking upon a 1-year effort to review their Television without Frontiers Directive.

Mr. SHIMKUS. And the French are really leading this crusade, are they not?

Mr. VRADENBURG. Historically, they have led the crusade, and of course the existing restrictions in Europe are that 50 percent, if practicable, of material over their broadcasting systems should be of European origin or at least not out-of-Europe origin. They are now discussing two additional potential restrictions. One is an investment quota, which basically would require their outlets inside of Europe to invest a certain percentage either of their revenues or of their programming expenditures on European productions. That would be a step beyond where they are today.

And the other restriction they are discussing is whether to try to extend, if they can find a way to do so, these quota restrictions onto the new media so that in fact video-on-demand systems or rather new media delivered systems might have a content restriction inside them. Both of those would clearly be steps, in our view, in the wrong direction. And as Ms. Richardson's pointed out, the irony here is that the Internet now gives the opportunity to European nations and cultures to distribute French products, Germany products, English products, Swedish products without any constraint on the means of distribution to American electronic consumers. So that in fact they have more opportunities to distribute their products in this country.

Going that direction of positively encouraging the adoption of their cultural products worldwide clearly is a much more productive way for the, we think, to develop not only their own economy but also to enrich the cultural experiences of American consumers, who now might have the opportunity to obtain access to very narrowly culturally tailored products that otherwise couldn't be managed on our American broadcast system or through our theatrical distribution system, but which may now be available through online distribution systems. So it seems to us that a more positive approach to promoting cultures, as opposed to trying to restrict other people's cultures, is now in order.

Mr. KOVAR. Cultural content restrictions by foreign governments would not be enforceable under the Hague Convention. The Hague Convention is intended to apply to private types of lawsuits. To the extent that private individuals seek to use private lawsuits to go after cultural content that they don't like and that may be somehow prohibited under local law, the convention would allow and would expect, frankly, our courts not to enforce that based on our traditional strong public policy in favor of First Amendment rights.

Mr. SHIMKUS. Thank you very much. And, Mr. Chairman, I will yield back my time.

Mr. STEARNS. The gentlelady from California, Ms. Harman?

Ms. HARMAN. Thank you, Mr.——

Mr. STEARNS. I am sorry, I beg your pardon, Mr. Gordon? Sorry. The gentleman from Tennessee is first.

Ms. HARMAN. If he is first, he should be first.

Mr. STEARNS. Yes.

Mr. GORDON. One quick question. I would like to learn more about the service versus goods argument, Ms. Richardson. I understand that within the content community that there is a debate now or at least a division. Could you tell me what is that division, and who is on first and second here?

Ms. RICHARDSON. Well, sorting out where people are at any given time is always a challenge, but I will certainly take a stab at it. The debate is whether a digitally delivered good or service should be benefiting from the rules of the GATT, which governs straight——

Mr. GORDON. Yes, I understand that.

Ms. RICHARDSON. Okay.

Mr. GORDON. What I am interested in is if there is a—I understand there is a division within the content industry for that reason that you are—that is basically telling our negotiators not to move forward. So who is on first and second here?

Ms. RICHARDSON. All right. The EU is clearly on one extreme end of this debate. They believe that all digital delivery of content should be classified as a service.

Mr. GORDON. Right. Are our domestic content providers all have the same position?

Ms. RICHARDSON. I think they are all on the same general page. We have——

Mr. GORDON. So what is the problem with—or do I misunderstand that you collectively have asked our negotiators not to move forward until there is a consensus opinion?

Ms. RICHARDSON. The EU has said they will not move forward until they get their way.

Mr. GORDON. Right, but——

Ms. RICHARDSON. We have said——

Mr. GORDON. [continuing] my question, though, and maybe I am—I am not trying to be tricky or anything——

Mr. VRADENBURG. No. Mr. Gordon, I think you are going to find most of the music and entertainment businesses in this country on exactly the same page, that the classification ought to be that of goods. The concern is moving forward and pressing our U.S. Government to move forward when they might lose that negotiating point with the European Union. This is more a United States versus EU issue than it is any significant division within our industries.

Mr. GORDON. Well, if the EU is basically winning by our non-action, what do we have to lose by going forward?

Mr. VRADENBURG. Well, I would take the view that in fact the EU is pressing and insisting that the classification of digitally delivered content be that of services and just taking that view. So if we were to move forward and close the issue now between the USG and the EU, it would be closed in the wrong direction. So we are hopeful that if we move forward with the marketplace, that we will

find out that in fact most of the products that are being delivered digitally in fact correspond to and replace hard goods products, and thus the case for the United States position will be stronger through time.

Mr. GORDON. So there is not a division then within our content industry here in this country.

Ms. RICHARDSON. I don't think there is a deep division. There are people that understand their business models better or less good who are more confident in drawing the line today. But I think all of us believe that there are many goods transactions, and there may be some services transactions. Exactly where that line should be drawn is hard to say, because the business models, at least in the film industry, are still developing.

Mr. GORDON. Thank you. I would like to yield the rest of my time.

Mr. STEARNS. Well, we are going to break and come back for more questions. Just, Mr. Gordon, I might also follow up on what you just said. What about software? How is software handled in terms of services or goods?

Ms. RICHARDSON. I believe that they believe that they have a foot in both camps, that the analog of a digitally delivered product is a product. There may be some new kinds of software services, but I am sorry, you should have spoken.

Ms. WAGGONER. No, that is okay. I think that we would say that there may be—they can be classified as both, and it really depends on the business model and the circumstances. And one way to begin to look at it, because this is still being debated within the industry, is the difference between purchasing something on a recurring cost basis or a non-recurring cost basis. So I think that there are products that are a good, and there are products that are service, and it is very complex. And the industry, as it moves forward with new business models, is going to have to sort this out.

Mr. VRADENBURG. I think we can't lose sight of the fact that this is not just a technical sort of debate here. There are major potential trade consequences to the classification issue, and clearly United States industries will be better off with the greater of the classification of these digitally delivered products as products, because there will be more protection under existing trade rules.

Mr. STEARNS. Okay. Well, the committee is going to come back and reconvene. And we will take a break now. Just we have two votes, so we have this vote, which is about 5 minutes left, and then we have another 5 minutes, so we should be back in about 12 minutes or so.

[Brief recess.]

Mr. STEARNS. The subcommittee will come to order. We have got a little time before the next vote, so I think we will start here. And I think the next member in line is the gentleman from New Hampshire. Mr. Bass is recognized.

Mr. BASS. Thank you very much, Mr. Chairman. Mr. Vradenburg, during my opening statement, I outlined my interest in being sure that we have considered these issues in the whole, the whole issue—how they are related to our domestic interstate trade policy and so forth. You seem to agree, at least I caught a

little nod. With respect to sales and use taxes and products classifications, can you explain how you think these matters are related?

Mr. VRADENBURG. Yes. We had the opportunity to serve on the Tax Commission that was formed by Congress a couple of years ago. And during the course of the debates of that Commission, it became clear that one of the critical elements in this debate was whether or not States and localities—State and locality taxing jurisdiction, from there are about 7,000 in this country, could tax out of jurisdiction sellers. Sellers that had no physical nexus to their jurisdiction and otherwise weren't doing business in their jurisdiction, could they impose a State or local sales or use tax obligation—collection obligation on those companies? And that is, of course, to some extent, the same debate that is going on with respect to Europe now and out-of-European sellers.

We urged, in the context of the State and local sales tax debate in this country, that there be a radical simplification of the tax collection obligations associated with collecting out-of-State seller transactions so that the costs of collections on that of State businesses would be significantly reduced. And then if that were the case, then in fact we could contemplate a system where in-State sellers and out-of-State sellers could pay equal State sales or use taxes, and there wouldn't be any differential treatment of different modes of distribution.

That same debate is now going on in Europe, where Europe at least only has 15 taxing jurisdictions at the moment, is trying to simplify their systems of taxation so that they can impose on out-of-European sellers some tax collection obligation, even though the seller is not within the boundaries of Europe.

Mr. BASS. Are you advocating—I just want to make clear your first point—that we have some sort of a national sales tax on Internet transactions?

Mr. VRADENBURG. No, not at all. We urge the States to go through a process of simplifying their State and local sales tax system, because you will upon examination that inside a State you may have 3 or 4 different rates, you may have 3 or 4 different classifications of the same product or service within a State, and certainly between States, and you had a variety of exemptions and administrative requirements. And so that most big corporations in this country doing business in many States will file over 100,000 State or local sales tax reports every year.

So what we were urging to the States is that they radically simplify their systems, that in fact the States adopt one rate per State, that they have one audit per State, that they have a single means by which they would classify goods or services sold within their State, and that we have an acceptable default rule on how to determine the residence of an Internet buyer so that we would not be subjected to the possibility of paying taxes in multiple States.

Mr. BASS. Is there any extension of that concept internationally?

Mr. VRADENBURG. Well, yes. The European Union is now considering a single point of registration with respect to out-of-European sellers. They have not yet settled on whether they are going to agree to that and, if so, whether they are going to have one or 15 different VAT tax rates depending upon the jurisdiction of the buyer. And if they have 15, how in the heck an Internet seller who

may simply be selling to a credit card, knowing he is selling somewhere in Europe, may not be able to determine which jurisdiction they are selling in.

So Europe is at least beginning to think through how to simplify their VAT collection tax systems. They are not there yet. We still have issues with Europe. We are still discussing the issue with Europe. But it is a species of the same issue as we are confronting here in the United States.

Mr. BASS. I bought something in Europe last fall, but I never knew, I never knew. I thought I was buying something in America, and I didn't know that it came from Europe until I got a—it arrived, and there was a—it was called the Stanley Company—sounds American to me. Did I pay any taxes on that?

Mr. VRADENBURG. You were probably obligated to pay a use tax in the jurisdiction in which you reside.

Mr. BASS. I couldn't even read it. I didn't know what jurisdiction it was.

One last question, because I am running out of time here. If this committee were to—subcommittee, rather, were to make some recommendations, either legislative or any other fashion, concerning this issue—this is for any of you who wish to comment on this—what should we do? I am sorry to be so vague, but I am just curious to know, as we try to understand what is a very complex issue, what role does this subcommittee have to play?

Mr. VRADENBURG. Well, I think the policy approach, how it gets translated into a statute-governed, domestic transactions or some position for the U.S. Government in international negotiations for Europe, I don't comment on. But the challenge here is to simplify the global system of tax collection. We cannot, over a long period of time, treat sales over the Internet differently than we treat physical sales within jurisdictions. It is neither fair and equitable nor appropriate. So at some point, we have to get to a system that does not discriminate based upon the form of distribution what the tax rate is.

But having said that, the costs of compliance to a company that is located in Canada to comply with 7,000 different State and local taxing jurisdictions in this country is overwhelming. And as a consequence, as a practical matter, you are never going to get tax compliance. So you need to simplify our domestic system, the State and local sales taxes without adopting a national sales tax but simplify it. And Europe has to simplify the VAT tax collection system so that in fact an Internet seller can register in one or a few places in the world and pay a tax rate based upon the jurisdiction into which his or her goods or services are sold.

Mr. BASS. Thank you, Mr. Chairman.

Mr. STEARNS. Yes. The gentlelady from California, Ms. Harman?

Ms. HARMAN. Thank you, Mr. Chairman. I would like to ask unanimous consent to put my opening remarks, which I was unable to deliver then, in the record.

Mr. STEARNS. By unanimous consent, agreed upon.

Ms. HARMAN. And I apologize to the witnesses for missing your testimony. As everyone knows, the scheduling around here is very difficult. I also have been trying to figure out what questions have

been asked so that I don't repeat, but I have a few that I think have not been asked yet.

Starting with Mr. Kovar, I would be interested if you could just highlight for us any differences of approach to these issues that this administration is taking over the administration of your predecessors. I don't think you address this in your testimony, and I don't think anyone has asked about it. I just would offer a comment, which I make all the time, which is that there are digital Members of Congress and analog Members of Congress, and we are not divided by party; we are divided by perspective. And I would like to hope that there are lots of digital members in this administration who think about these issues the way many of us do.

Mr. KOVAR. The simple answer, Ms. Harman, is that I haven't seen a real change at this point.

Ms. HARMAN. Does that mean you haven't seen any evidence of a change yet or you predict the same focus will be kept?

Mr. KOVAR. Well, I think I would be out of line if I tried to predict. But so far the approach to these negotiations hasn't changed since the new administration came in.

Ms. HARMAN. Okay. Well, let me say that I hope—I can't recall every single thing the last administration did, but I certainly saw some wrestling there with tough issues. Would anyone on the panel like to comment? Have any of you noticed something different that is either good or bad in terms of a focus on some of these issues? No. Okay.

Moving along, I think a gut issue here, and it related to the digital divide and to a lot of things we all worry about, is how do we get more people around the world online? And I think that is a goal everybody shares. What thoughts do you have? It relates to cost of getting online. It relates to access to equipment. I would love to hear an answer from my good friend, Mr. Vradenburg.

Mr. VRADENBURG. Thank you, Ms. Harman. The main issue is cost for the sake of simplicity. Just as an American consumer who may be analog but thinking about going digital, one of the first questions asked is how much does it cost, and what is the value of moving from analog to digital? I think the challenge around the world is to extend information and communications technology systems to make them more affordable and to sort of blow them out, so to speak.

And that means getting privatization of national telephone companies, getting increased competition to those phone companies, intelligent, wireless spectrum policies on the part of lesser developed countries on the view that, in fact, electronic access to developed markets is going to be a lot cheaper than is physical access to developed markets, and that the lesser developed nations of the world and the developing nations of the world should be finding ways to make more universal and affordable their telecommunications systems.

Certainly, in my recent visits to China, there is an enormous appetite on their part to do just that, to blow out their telephone system to many more people, to make it more affordable so that their electronic sellers can get access to the electronic buyers here in this country.

Ms. HARMAN. Well, I totally agree with that answer. Are there steps that we can take in terms of legislation or focus? Are there world fora that we could encourage this committee, this Congress, that would be useful? I mean should we be gearing toward some sort of convention on this the way there is WIPO and other conventions on other issues that relate to this worldwide digital economy?

Mr. VRADENBURG. Well, I would urge that Congress and individual Congress men and women urge the United States Trade Rep to make this a high item on his agenda. Beyond that, there is a whole series, sectors of industries that are engaged in the electronic commerce value chain whose costs and/or competition would be enhanced—advertising services, financial services, air transport services, express delivery services. There are a whole range of sectors in the service sector, which, if liberalized and the cost reduced as a consequence, would significantly expand electronic commerce.

Ms. HARMAN. Other comments? Ms. Richardson.

Ms. RICHARDSON. I would like to address that point too. As George's testimony said, trade promotion authority gives the administration tools to negotiate on our behalf. There are mechanisms in the services agreement that can get to cost-based issues for infrastructure. There are certainly mechanisms in the trade system that can keep the content open.

One of the few things that customers are willing to spend money for to help pay off the expensive cost of infrastructure is entertainment. That cost can be artificially jacked up if countries start putting content restrictions on delivery of content over the Internet.

Ms. WAGGONER. And I would just underscore that point as well, and there are a number of bilateral agreements as well as regional agreements and negotiations that are occurring. So as we consider TPA, I think setting out clear negotiating objectives to cover digital trade in some of these issues would be very important.

Ms. HARMAN. Well, I see my time is up. I thank you all for that answer. Mr. Chairman, I would just like to suggest that part of our jurisdiction in this subcommittee, I believe, is to perhaps make constructive suggestions to our administration about proceeding with some of these things. If that happens, I would see it as a win-win-win for our country, for other governments, and for consumers around the world.

Mr. STEARNS. You are welcome to stay. We are going to have probably another second round here if members—the gentleman from—Mr. Joe Pitts has left, okay.

Well, let me ask Mr. Kovar something, and I will take 5 minutes, and Mr. Bass and Ms. Harman, you are welcome to ask a second round of questions. Here, June 6 is the negotiations you start. Without putting yourself in some kind of secret presentation here, can you sort of walk us through the changes that the U.S. is seeking for this June 6 negotiation and what changes, particularly in a broad sense, you might think are necessary?

Mr. KOVAR. Well, at the broadest sense, what we would like to do is to replace the existing text, which is overreaching. It tries to do too much.

Mr. STEARNS. All of the existing text?

Mr. KOVAR. Well, not all of it, but essentially the jurisdiction section of it we think ought to be replaced with a simpler approach

to jurisdiction that doesn't try to do so much. It would probably have fewer types of jurisdiction in the required area where you actually get enforcement, and it would have a narrower section on prohibited jurisdiction. And it would allow for more flexibility in the middle for national practices to continue. That is what we would really like to see, is a new text to emerge where the jurisdiction provisions are simpler.

We think on the recognition and enforcement side of the convention that the convention is in pretty good shape. I mean there is still work to be done there on individual things, but that overall it is in pretty good shape. Then there is a number of other issues that are related to the convention—the connection between this convention and Europe law, whether we need a mechanism for applying piece meal to different countries depending on whether their legal systems are good enough, to permit enforcement of their judgments. And those are issues we would like to see start to be tackled in this June session. But we think the jurisdiction aspects are the most important.

Mr. STEARNS. We have recognized foreign judgments here in the United States, but other countries sometimes are unwilling to do so. How will the convention benefit U.S. companies and consumers seeking to enforce judgments overseas?

Mr. KOVAR. Well, we hope that we ultimately will get a convention that has simpler rules of jurisdiction that can attract widespread support, and that we can stop having such an excessive focus on them. We won't raise as many difficult problems as we have got today. And then we will be able to move right to the recognition and enforcement side of the convention, which is where we think we can level the playing field for American litigants.

The enforcement side of the convention now has rules that are very similar to the rules that are enforced in the State of Florida, for example, or the State of Illinois, most States in this country that have the Uniform Act or that use the common law. And what we most hope to have is an international system under this convention that applies those rules in most of the major trading countries of the world.

Mr. STEARNS. Ms. Waggoner, I understand that there is a WTO Work Program on electronic commerce that was formed to examine trade-related electronic commerce issues. I guess the question is do you know what progress has been made in addressing the concerns that you even mentioned in your testimony?

Ms. WAGGONER. Yes. Well, given that we have not been able to launch a new round, we have been in a holding pattern, we, of course, continue to support that Work Program, and we are looking forward to moving the agenda, and we continue to work through ITI. We have been educating the WTO delegations on the importance of e-commerce, and we continue to work with those delegations to educate them, to help them push forward so we can build support for a new round and for this component of the new round.

Mr. STEARNS. Tell me worst case scenario. Tell me what—you mentioned in your testimony that the Government should refrain from enacting trade-related measures that impede e-commerce. What specifically things are you concerned about?

Ms. WAGGONER. Well, I think one of the questions that we have been talking about today is the issue of how to classify an item.

Mr. STEARNS. Problems.

Ms. WAGGONER. So I think that if you classify prematurely goods versus services, you could certainly damage the growth of e-commerce. I think if you have a regulatory environment, particularly in telecommunications, a regulatory environment that hinders market growth but does not force privatization, particularly in the developing nations, those things could definitely hinder growth in new markets in the developing countries.

Mr. STEARNS. What about in the area of Latin America? How crucial is the FTAA to opening up telecommunications in Latin America?

Ms. WAGGONER. I think it is very critical. I think that we are going to have to have trade promotion authority in order to force some of those recalcitrant countries to move. They are unwilling to make concessions if they are not certain how they are going to be treated when we bring the agreement back home. So I think——

Mr. STEARNS. You are talking about Fast Track?

Ms. WAGGONER. Fast Track, that is correct.

Mr. STEARNS. You don't think we can get it done without Fast Track for the——

Ms. WAGGONER. I think it is going to be difficult.

Mr. STEARNS. That is a new name for it, trade——

Ms. WAGGONER. Trade promotion authority.

Mr. STEARNS. [continuing] promotion authority.

Ms. WAGGONER. Correct.

Mr. STEARNS. In the new terminology in Washington, when you are trying to pass something, if you have trouble, you change the name.

Ms. WAGGONER. Change the name.

Mr. STEARNS. Well, my time is expired. Mr. Towns?

Mr. TOWNS. Thank you very much, Mr. Chairman. Mr. Kovar, what is the State Department doing to encourage other nations to sign the WIPO Treaty's Copyright Act, which further protects intellectual property? What are they doing? What is the State Department doing?

Mr. KOVAR. Mr. Towns, I am not the right person to answer your question, and I apologize for that. I am sure it is something that we are handling through the right channels, and there are other agencies that are also involved, including the Commerce Department.

Mr. TOWNS. Okay. Well, I accept that. I am just sitting here thinking when we look at what is really going on and you think about the problems around these issues that—we are not letting anybody come in and steal our oil or steal our cash. We just wouldn't allow it. And then when I looked and listened as to what is going on here, I think that we have some serious problems.

But let me ask you one other question. In light of your remarks earlier about the critical importance of tax policy for e-commerce, what do you think of the EU's proposed change to their tax system with respect to e-commerce? I think Mr. Vradenburg, really I wanted.

Mr. VRADENBURG. Well, we don't think that yet it is adequate. It is basically proposing that there be a single point of registration, but still 15 different taxing rates. They are not yet committing to move toward a harmonized VAT rate across Europe, although I think that may be inevitable because of their monetary integration. And they are not yet undertaking to exempt smaller transactions or accumulate smaller transactions. So there are a number of respects in which we think that their proposals are inadequate in terms of simplifying their system sufficiently to justify out-of-jurisdiction—imposing tax collection obligations on out-of-jurisdiction sellers.

This is a species, Mr. Towns, of a problem that is being created by the Internet, or a challenge being created by the Internet in a lot of areas. The Internet is global in character. And as a consequence, there are people that are outside the jurisdiction of any national government who are either conducting electronic commerce transaction and thus not within the jurisdictional reach of that government for tax collection purposes or who may be doing something that is committing a tort within a jurisdiction and in fact not within the jurisdiction of any—the Nation in which the tort occurs.

So these issues are going to have to be dealt with, but they are big issues. They are not issues which I think we can deal with with tweaks to the existing system. Mr. Kovar here has been handed the challenge of trying to deal with this issue in the context of jurisdiction. We are trying to deal with it in the context of taxes. We are also trying to deal with it, obviously, in the context of copyright enforcement around the world.

But this whole challenge of a global system of distribution and communications, when each nation is, by definition, not global in character, is a challenge we are going to confront for the next 5 to 10 years, and we have to take the cautious approach that my private sector colleagues on my left, your right, are advocating with respect to jurisdiction.

But we have got to deal with these problems. We can't ignore them. They are not going to go away; they are only going to get worse. And so that we have to confront them head on. And the tax issue is one that you have raised, Mr. Bass has raised, and the jurisdiction is a question that all of the members of the panels have raised. And they are very important issues that we have to got to deal with.

Mr. TOWNS. What do you suggest that the Congress do at this time?

Mr. VRADENBURG. Well, on the domestic tax issue, where clearly the Congress does have jurisdiction and is now discussing the question of State and local taxation of Internet sales, we would urge the Congress to embrace a revision of the existing Internet Tax Freedom Act, which would encourage the States to simplify their State and local taxation systems to reduce the cost of tax collection on out-of-State sellers as a component of the extension of the existing moratorium, which bars Internet access taxes and also bars discriminatory taxation of the Internet. So in that context, we would urge that as Congress takes up this subject, as it must by the time that the existing tax moratorium expires this October, confront the

issue of incenting the States to simplify their State and local taxation system on this score.

Mr. TOWNS. All right. Thank you very much. I yield back.

Mr. STEARNS. The gentleman from New Hampshire.

Mr. BASS. Yes, thank you, Mr. Chairman.

Mr. TOWNS. I yield back.

Mr. STEARNS. Sure. Go ahead.

Mr. BASS. Thank you, Mr. Chairman. Mr. Kovar, will the Hague Convention result in U.S. firms being subject to foreign jurisdictions and facing enforcements or otherwise be regulated in ways that they are not today?

Mr. KOVAR. It shouldn't. Today, American corporations are subject to jurisdiction around the world under local law, and most countries' jurisdictional laws are, in some cases, broader than American jurisdictional rules. And those same countries are subject to enforcement of that judgment back home in the various States of the United States. So if we get the provisions right, it shouldn't really—it shouldn't change things coming into the United States, but we hope it changes things going out of the United States.

Mr. BASS. One final follow-up for Mr. Vradenburg, not for you. You made reference in my earlier round about—or at least some reference—about the issue of defining jurisdictions. But some of the others of you, Ms. Wellbery and some of the others have also mentioned, talked about this in your testimony. Is there any easy solution, from your perspective, to the issue of defining jurisdictions for e-commerce transactions?

Ms. WELLBERY. I don't think there is any easy solution. Our traditional means for defining jurisdiction are all based on physical location, either of the actors or of the transaction or where the goods were delivered. And none of those things are necessarily relevant in the e-commerce world, because, as we all know, there is no there there; it is happening in cyberspace. And I think that is really—we are talking about the same issue in a number of contexts—in the tax context, in the jurisdiction context. The real problem is figuring out how to identify where these transactions are taking place, and if we can't, what system do we put in the place of the system we used to use?

Mr. BASS. Well, if nobody else has any comments, I will yield back.

Mr. STEARNS. Okay. The gentleman yields back.

Let me just conclude by saying that the United Kingdom has just come out with sort of, I guess, a bombshell talking about the EU VAT Tax Directive. Were any of you familiar with that? They have come out saying there should be no VAT tax on this. Are you familiar with that, George? No? No. Okay. Well, I think this goes to the heart of how difficult it is to see what we are going to do. And this committee is going to try and have some type of legislation dealing with continuing the moratorium here until we figure it out.

A thought I had was the taxation on your telephone, your wireless telephone, either whether it is abroad or whether it is in the United States, we work that out. So that might be a paradigm for someway to do this. In States like mine where we have no State income tax, we rely heavily on sales tax. That can't go on, because the bricks-and-mortars versus the bricks-and-clicks are going to

have a hard time. And so we somehow got to come up with a solution to this, and I am sure Governor Jeb Bush is going to be on top of us to—he won't be happy with this moratorium, but, again——

Mr. BASS. Well, if the gentleman would yield——

Mr. STEARNS. Yes.

Mr. BASS. [continuing] the obvious solution for Florida is to not have either a sales or an income tax, like the great Granite State of New Hampshire.

Mr. STEARNS. That is a good possibility.

Well, I want to thank all of you for waiting while we voted and also for attending. And I thank all of you in the audience. The subcommittee is adjourned.

[Whereupon, at 4:03 p.m., the subcommittee was adjourned.]