THE INTERNATIONAL ECONOMY
THE MAGAZINE OF INTERNATIONAL ECONOMIC POLICY
888 16th Street, N.W.
Suite 740
Washington, D.C. 20006
Phone: 202-861-0791
Fax: 202-861-0790
www.international-economy.com
editor@international-economy.com

Trade *and the* Internet

The risks and challenges of this new technology.

BY SUSAN ARIEL AARONSON

In its relatively short history, the internet has morphed from a source of information to a multidimensional market for goods, services, and ideas. One quarter of the world's people search for jobs and spouses, share information, and learn new skills on the web. The internet has increased economic growth, expanded access to information, and improved the rule of law within and between nations. In so doing, the information superhighway has altered what and how we trade as well as who we trade with. Not surprisingly, the internet has become an issue for trade negotiators. Policymakers have struggled to ensure that trade policy keeps pace with web developments.

Unfortunately, at the same time the internet has provided these positive benefits, the information superhighway has also become a battlefield. Firms, government agencies, and individuals probe each others' websites, and they also seek protection from privacy violations, data theft, counterfeit and rogue web sites, and computer intrusions. Democratic and authoritarian governments alike use "security software" to restrict and even disrupt the free flow of online information. In so doing, these states may make the web more secure but they may also undermine privacy rights and freedom of expression for net users (netizens). Although U.S. and European firms are often the principal defenders of an open internet, U.S., Canadian, and European firms provide much of the infrastructure as well as censor ware or blocking services to their home governments and to repressive states such as Iran, Russia, and China. In short, Western business has become both a demandeur of an open internet as well as a supplier of tools to censor it. Not surprisingly, trade policy reflects that contradiction.

Policymakers are struggling to define a clear and universally accepted set of rules to maintain an open and secure internet. The United States provides an example of policy incoherence. In May 2011, the United States announced an official International Strategy for Cyberspace. In July 2001, the Defense Department released its cyber strategy, noting that the U.S. military would defend U.S. networks while taking offensive actions (such as probing) when needed. But the United States has not clearly defined when it can/will attack and which entities—governments, firms, civilians—will be warriors in this fight. Such clarity is important because in most NATO countries, the military depends on the private sector to provide energy, transportation, telecommunications services, and financial infrastructure.

In recognition of this close relationship and in response to Chinese (and other government) cyberattacks on nongovernmental entities such as firms and universities, the United States now requires all publicly

Susan Ariel Aaronson is an Associate Research Professor at George Washington University, and a Research Fellow at the World Trade Institute.

STATE DEPARTMENT PHOTO BY MICHAEL GROSS

The United States also leads a global effort to help dissidents undermine government efforts to suppress citizen voices or access to information. U.S. Secretary of State **Hillary Clinton** has given numerous speeches arguing that internet freedom is a key element of U.S. foreign policy.

—S. Aaronson

traded companies to disclose material cyber risks (risks that could present a severe financial threat to the firm.) These risks could include security breaches, deliberate attacks to steal assets, intellectual property, or hacker efforts to disrupt operations. Thus for the United States, internet security is now a national security issue.

U.S. trade policies also send a mixed message. On the one hand, the United States has taken many steps to ensure an open internet. Policymakers proposed language in the Transpacific Partnership (a trade agreement being negotiated by nine countries bordering the Pacific) to prohibit signatories from blocking internet data flows and from establishing local infrastructure mandates for digital service providers. The United States also leads a global effort to help dissidents undermine government efforts to suppress citizen voices or access to information. U.S. Secretary of State Hillary Clinton has given numerous speeches arguing that internet freedom is a key element of U.S. foreign policy. In addition, the U.S. government helped to establish the Global Network Initiative, a multisectoral partnership among business, human rights groups, academics, and other interested parties. The Initiative has developed principles to guide the information technology industry on how to respect, protect, and advance freedom of expression and privacy when faced with government demands for censorship and disclosure of users' personal information.

On the other hand, the United States is negotiating agreements and devising policies that could reduce internet freedom. According to the U.S. Trade Representative, the Anticounterfeiting Trade Agreement, signed by the United States, Australia, Canada, Korea, Japan, New Zealand, Morocco, and Singapore on October 1, 2011, is designed to "address the problem of infringement of intellectual property rights in the digital environment…in a manner that balances the rights and interests of the relevant right holders, service providers, and users." But some observers note that in fact, it could hold service providers liable for criminal cyber activity by their business and individual customers. Moreover, the U.S. Trade Representative is studying whether it could challenge Chinese internet restrictions as a violation of international trade rules. However, the United States is unlikely to take this route, as policymakers would not want to create precedents that could limit the ability of the United States or its allies to restrict access to the internet for national security reasons. Finally, Congress is considering bipartisan legislation that would allow the U.S. Department of Justice, as well as copyright holders, to seek court orders against websites accused of enabling or facilitating copyright infringement. Some critics fear that the bill, as currently written, could undermine user-generated content, freedom of expression, and existing policies of determining copyright and privacy.

The information superhighway has also become a battlefield.

How can policymakers achieve the right balance of internet security and freedom and make that framework enforceable globally? At first glance, the World Trade Organization might be the most appropriate regulatory platform. One hundred and fifty-five member states have committed to respect WTO principles. The WTO's General Agreement on Trade in Services (GATS) covers some internet-related trade issues, and includes provisions that could effectively balance internet openness and security. The agreement recognizes that there are times when nations would need to censor or block products or ideas at their borders. But the GATS also states "the public order exception may be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society."

But the WTO might not be the most effective venue to balance internet freedom and security. First, the GATS regulates the behavior of states, not individuals or firms. Individuals and firms have no way to directly represent their interests. Moreover, although transparency is a principal norm of the WTO, its agreements say nothing about data privacy, human rights, or cyber security. Negotiations among member states often take years, and are kept secret unless member states choose to reveal their positions. In general the public is uninvolved in and uninformed about WTO negotiations, agreements, and day-to-day activities.

Continued from page 76

Hence it appears that the internet culture of universal access, open standards, freedom of expression, and no control is at odds with the culture of the WTO.

If the WTO is not the best regulatory platform, policymakers might turn to the internet to develop a new regulatory approach that allows open and secure access, encourages innovation, protects freedom of expression, and respects the privacy of web users. They might consider "crowd sourcing," asking interested parties to develop and assess alternative ideas. Crowd sourcing can be problematic, as crowds can turn into lynch mobs or rely on uneducated opinions. But crowd sourcing can also transcend individual bias and foster creative compromise and responsible decisionmaking. Policymakers have already turned to crowd sourcing to review patents and to gain public comment on the proposed AT&T/T-Mobile merger. This strategy may also build public support for a new approach to internet governance—having participated in the development of these policies, the public may feel greater ownership of them. Ironically, net values of open standards, freedom of expression, and universal access might help officials develop not only a new approach to trade policymaking but better accepted trade policies to govern the internet. ◆