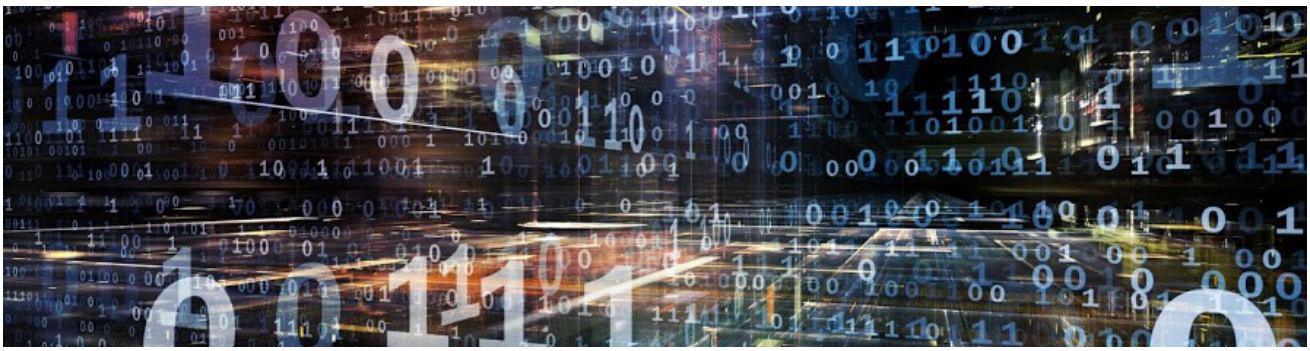
ICTSD
International Centre for Trade and Sustainable Development

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

The E15 Initiative

STRENGTHENING THE GLOBAL TRADE AND INVESTMENT SYSTEM FOR SUSTAINABLE DEVELOPMENT



Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows

Usman Ahmed and Anupam Chander

November 2015

E15 Expert Group on the Digital Economy

Think Piece

ACKNOWLEDGMENTS

Published by

International Centre for Trade and Sustainable Development (ICTSD)
7 Chemin de Balexert, 1219 Geneva, Switzerland
Tel: +41 22 917 8492 – E-mail: ictsd@ictsd.ch – Website: www.ictsd.org
Publisher and Chief Executive: Ricardo Meléndez-Ortiz

World Economic Forum
91-93 route de la Capite, 1223 Cologny/Geneva, Switzerland
Tel: +41 22 869 1212 – E-mail: contact@weforum.org – Website: www.weforum.org
Co-Publisher and Managing Director: Richard Samans

Acknowledgments

This paper has been produced under the E15Initiative (E15). Implemented jointly by the International Centre for Trade and Sustainable Development (ICTSD) and the World Economic Forum, the E15 convenes world-class experts and institutions to generate strategic analysis and recommendations for government, business and civil society geared towards strengthening the global trade and investment system for sustainable development.

For more information on the E15, please visit www.e15initiative.org/

Usman Ahmed is the Head of Global Public Policy at PayPal, Inc. Anupam Chander is Professor of Law at the University of California, Davis.

With the support of:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Canada

And ICTSD's Core and Thematic Donors:

Department for International Development

SWEDEN

Ministry of Foreign Affairs

Ministry of Foreign Affairs of Denmark
Ministère des Affaires étrangères du Danemark

Ministry for Foreign Affairs of Finland

Citation: Ahmed, Usman and Anupam Chander. *Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows.* E15Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, 2015. www.e15initiative.org/

The views expressed in this publication are those of the authors and do not necessarily reflect the views of ICTSD, World Economic Forum, or the funding institutions.

ISSN 2313-3805

ABSTRACT

This paper addresses the question of whether it is possible to balance the need for a free flow of information across borders with legitimate government concerns related to public order, consumer privacy, and security. The paper begins by highlighting the risks associated with limitations on free information flows and the policy concerns that lead to these limitations. The paper then provides an analysis of the current international regime on cross-border information flows. The authors argue that specific binding trade language promoting cross-border flows— combined with continued international cooperation — will enhance, rather than undermine, public order, national security, and privacy.

CONTENTS

LIST OF ABBREVIATIONS

EU	European Union
GATS	General Agreement on Trade in Services
KORUS	U.S.-South Korea Free Trade Agreement
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
SPS	Sanitary and Phytosanitary
TISA	Trade in Services Agreement
TPP	Trans-Pacific Partnership
TTIP	Transatlantic Trade and Investment Partnership
US	United States
WTO	World Trade Organization

INTRODUCTION

The newest battleground in international trade is over the flow of information. Governments seek to exercise control over data flows as part of their broader efforts to assert what they see as "digital sovereignty." Some governments believe that the free flow of information poses a threat to public order, consumer privacy, or national security. Privately, many governments also worry about the competition for domestic businesses from foreign service providers, especially in domains traditionally insulated from foreign competition. In response, excessive government assertions of national borders in cyberspace may "balkanize" the Internet and erode the enormous benefits of this global medium. This tension raises a crucial question: is it possible to balance the free flow of information across borders with legitimate concerns related to public order, consumer privacy, and security?

The importance of the free flow of information across the world is difficult to overstate. The free flow of data, including across borders, is a key part of what makes the Internet the powerful force for information and economic development that it has proven to be over the past two decades.[1] McKinsey sees the Internet as "the great transformer," accounting for one-fifth of GDP growth in developed countries.[2] Perhaps McKinsey's most surprising conclusion is that "[m]ost of the economic value created by the Internet falls outside of the technology sector, with 75 percent of the benefits captured by companies in more traditional industries." As McKinsey describes, traditional industries benefit from "increased productivity, opportunities to expand into domestic and foreign markets, the means for radical product development, and the rapid deployment of game-changing ideas."[3] These game-changing ideas can be rapidly deployed globally, which is why digital trade has become a key part of modern economies.

The significance of the free flow of data becomes even more apparent when taking into account the crucial role of such flows in enabling the most recent technological innovations. Consider the following 10 innovations that rely on information flows:

1. **The Internet of Things.** Devices like an Apple Watch or a Samsung Smart TV — or even a Caterpillar or Komatsu heavy machine — depend on the flow of information across national borders to gather and process data.

2. **App Economy.** Individuals and small companies can now build applications and leverage global marketing, distribution, and payments networks to sell their products and services to the nearly 2 billion smartphone users across the world.[4]

3. **Outsourcing of Services.** The ability to outsource business processes and information technology services depends on the cross-border flow of information.

4. **E-commerce.** Companies like Alibaba and eBay depend on global information flows to enable people to sell to, and buy from, global markets.

5. **Cloud computing.** Cloud computing depends on the transfer of large volumes of information, often across borders, to server farms typically located based on network efficiencies, security, and costs. Robots, for example, increasingly depend on cloud-based information storage and processing.

6. **Big data.** Data sets can be larger if they include people across borders; analytics are often performed using tools and companies located in foreign jurisdictions.

7. **Digital products and streaming services.** Digital music and video services, from Apple, Netflix, Spotify, and others, increasingly allow customers across the world to download or stream audiovisual content.

8. **Social media and websites generally.** Social media, and the Web generally, implicate significant information sharing across borders.

9. **The sharing economy**. AirBnB, Uber, and the like allow one to share one's resources, for a price, with people from anywhere in the world.

10. **Crowdfunding**. People planning new projects can now raise funding from supporters across the world.[5]

This list demonstrates what is at risk if the free flow of information across national borders is eroded.

---

1 Business Roundtable, Putting Data to Work: Maximizing the Value of Information in an Interconnected World, Jan. 2015, http://businessroundtable.org/sites/default/files/reports/BRT%20Putting DataToWork.pdf

2 McKinsey Global Institute. Internet matters: The Net's sweeping impact on growth, jobs, and prosperity, May 2011; McKinsey Global Institute. The great transformer: The impact of the Internet on economic growth and prosperity, Oct. 2011.

3 McKinsey, Internet Matters at 7.

4 See, e.g., Kushner, David. "The Flight of the Birdman: Flappy Bird Creator Dong Nguyen *Speaks Out,*" Rolling Stone, Mar. 11, 2014, http://www.rollingstone.com/culture/news/the-flight-of-the-birdman-flappy-bird-creator-dong-nguyen-speaks-out-20140311#ixzz3gl1tVGLO; Curtis, Sophia. "Quarter of the world will be using smartphones in 2016," *The Telegraph*, Dec, 11 2014.

5 See, for example, http://www.engadget.com/2015/07/18/shenmue-3-kickstarter-record/.

Data localisation (requiring that Internet content providers store their data in country) and other barriers to cross-border flows of information tear at the fabric of global cyberspace. Information services that might have been supplied globally now must build out or pay for national data infrastructures in the countries in which they operate, carefully separating their services by country rather than offering a global service. This dramatically raises the costs of those services, often making them uneconomic to provide, particularly in the case of small- and medium-sized businesses.

Equally important, the free flow of information across borders not only benefits economic development and technological growth, but also supports free expression, as political dissidents often rely on foreign speech platforms to disseminate information.[6]

Even with these clear benefits of free flows of information, many governments have sought to curb these flows. The next section describes such efforts.

GOVERNMENT CONCERNS ABOUT DATA FLOWS

The Internet was developed largely without paying much heed to borders. But, even in the Internet's early days, governments found reasons to assert themselves with respect to cross-border flows of information. Authoritarian governments, in particular, fretted about the loss of control over speech they had previously exercised with respect to traditional media, such as newspapers, radio, and television. Even liberal governments sought to interfere with information flows when those flows ran afoul of national laws related to hate speech. A French court ruled that Yahoo! Inc. violated French law when it did not halt the auction of Nazi materials to a French audience. An effort in the United States (US) to target "foreign rogue websites" hosting copyright infringing content (the Stop Online Piracy Act) would have interfered with the domain name server system and potentially threatened the security of the Internet.

Some governments see the free flow of data across borders as a threat to national security, with reports about the National Security Agency (NSA) surveillance program arguably justifying those fears (though the NSA's reach is hardly contained in the US). Governments are also concerned about the threat to consumer privacy, when services gather personal data without consent and then use that data in a variety of ways around the world. Governments are driven also by the competitive challenge that the Internet poses to domestic businesses, owing to the ability of an Internet-based competitor to efficiently deliver products or services. Finally, some governments see the Internet as a threat to national efforts to control information, owing to its nature as a global platform for speech.

Increasingly government concerns over cross-border flows of information take the form of mandates for what has come to be called "data localisation"—efforts to keep information from leaving its home country. These mandates range widely. Australia, for example, requires that personally identifiable health information not leave the country without the consent of the individual to whom it pertains. British Columbia and Nova Scotia prevent personal information held by government agencies from leaving Canada without the consent of the data subject. The European Union (EU) permits personally identifiable information to leave the Union only under certain conditions, and it is considering tightening those conditions. Russia has begun putting in place a strict data protection regime, requiring that companies keep personal information of Russians in the country.[7] The Russian rules apply, for example, to Netherlands-based travel website Booking.com, which, according to the Russian authorities, "accumulates a large database of personal data of our citizens."[8]

Such national regulations around the world require information service providers to locate servers or other physical infrastructure in country in order to provide services.[9] These requirements result in the de facto blocking of information, as many firms, particularly smaller ones, are unable to locate servers in countries around the world.

6 Freedom of expression across national borders is one of the rights protected by the International Covenant on Civil and Political Rights, Art. 19(2): "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." On the importance of foreign speech intermediaries to dissidents in repressive states, see Chander, Anupam. "Googling Freedom," 99 *Calif. L*. Rev. 1, 2011.

7 Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde, Data Localisation in Russia: A Self-imposed Sanction. *ECIPE,* 2015. http://www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf.

8 Kurochkin, Dmitry, Marat Agabalyan and Saglara Ildzhirinova, of Dechert Russia LLC, Moscow, "Russia's New Server Localization Law: Implications for Foreign Companies," *World Data Protection Report,* Feb. 2015.

9 Chander, Anupam and Uyen P. Le. "Data Nationalism," 64 *Emory Law Journal* 677, 2015.

THE CURRENT INTERNATIONAL REGIME FOR CROSS-BORDER DATA FLOW

Early international interventions on data processing recognized the importance of both privacy and cross-border data flows. In 1984, an executive at American Express described transnational data flows as the "lifeblood of virtually every major economic activity."[10] In its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Organisation for Economic Co-operation and Development (OECD) noted the need for privacy protection amidst the development of vast databases, but also worried that "disparities in national legislations [on privacy] could hamper the free flow of personal data across frontiers." The OECD recognised that "transborder flows of personal data contribute to economic and social development" and that "domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows." The Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) required state parties to enact laws to protect privacy. At the same time, Convention 108 prohibited any party from "prohibit[ing] or subject[ing] to special authorisation transborder flows of personal data going to the territory of another Party." While open to all states for membership, Convention 108 remained exclusively European, until the addition of Uruguay as a member state in 2013.

The WTO, by contrast, counts most of the countries of the world as members. When the WTO came into being in 1995, the Internet was in its relative infancy as a global communications platform. The General Agreement on Trade in Services (GATS), negotiated in the early 1990s, did not explicitly deal with data flows across borders. The focus, instead, was on the general provision of services across borders and across multiple modes of service provision. Yet, the characterisation of how services might be provided across borders—including "cross-border supply" and "consumption abroad"—makes clear that the cross-border supply of information services was intended to be encompassed by GATS.

Indeed, the first WTO decision focused on GATS makes this clear.[11] In *United States – Gambling,* the WTO's Appellate Body ruled that US rules barring the cross-border supply of Internet-based gambling services were subject to the services liberalisation obligations of GATS. The US argued that even so, its rules were necessary to prevent underage gambling and to reduce fraud and money laundering and were thus an exception to the GATS obligations as a regulation of public morals. The WTO sided with Antigua in part, because US-based gambling services were treated differently from Antiguan Internet-based services and authorized Antigua to engage in limited retaliatory sanctions against the US. The application of the WTO agreements to information services is further confirmed in the WTO's ruling in the *China – Publications and Audiovisual Products* dispute. There, the US challenged a number of Chinese restrictions on the distribution of certain publications and audiovisual products, restrictions designed ostensibly to serve Chinese state censorship requirements. China argued that the electronic distribution of audio products was not covered by the agreement, but the Appellate Body concluded that China's commitment "would encompass distribution in electronic form."[12] The WTO went on to conclude that the Chinese restrictions were barred by that country's free-trade commitments.

Whether GATS applies to a particular measure that might restrict information flows depends on whether the country applying that measure has scheduled a relevant liberalisation commitment. Some 77 WTO members have made commitments on "data processing," but the scope of these commitments is not entirely clear, because computer-mediated services can be characterised in multiple ways, some of which might be liberalised and others not.[13] It could be argued, for example, that an accounting service provided online should not be considered "on-line information or data processing" when there is a separate category for "accounting services."

The GATS provides that states might impose measures that would otherwise run afoul of the agreement if necessary to comply with laws protecting the privacy of individuals.[14]

10 Drake, William. "Territoriality and Intangibility: Transborder Data Flows and National Sovereignty," in Beyond National Sovereignty: International Communications in the 1990s, edited by Kaarle Nordenstreng and Herbert I. Schiller, 259, 271, 1993.

11 Burri, M. & Cottier, T. Introduction: Digital technologies and international trade regulation, in Trade Governance in The Digital Age, p. 4, 2012.

12 China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, Dec. 21, 2009, ¶ 377. Chander, Anupam. The Electronic Silk Road: How the Web Binds the World in Commerce 156, 2013.

13 Berry, Renee and Matthew Reisman, Policy Challenges of Cross-Border Cloud Computing p. 22 (US International Trade Commission, May 2012) (noting that 60 countries have commitments on "on-line information and/or data processing," while 76 have commitments in for data processing). Our own review suggests that there are as many as 77 countries with "CPC 843" commitments for data processing services, though some of these commitments may be narrower than all data processing services.

14 General Agreement on Trade in Services, Art. XIV(c)(ii).

This exception to the free-trade obligations under GATS, however, will likely be interpreted narrowly so as not to undermine the agreement. After all, it is easy to claim that privacy can be protected only if information remains within a country, but it is much harder to demonstrate that this is necessary to protect privacy, an issue to which we return in Section 5 below.

HOW 21ST CENTURY AGREEMENTS WILL ADDRESS CROSS-BORDER FLOWS OF INFORMATION

The issue has also found its way into recent debates outside the WTO. The European Court of Justice has considered issues of cross-border Internet gambling provided from within the EU, but has been inconsistent in requiring liberalisation of trade.[15] With the US-South Korea Free Trade Agreement (KORUS), the US began asking its trading partners to explicitly affirm the value of the free flow of information. KORUS states: "Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders." While the language is hortatory, it still provides a basis for political pressure in case of noncompliance.

There are several trade agreements currently being negotiated that will likely incorporate language designed to safeguard cross-border information flows from national protectionist barriers. Because of their focus on such contemporary issues, these agreements have been described as "21st century trade agreements." While the negotiations are ongoing and secret, both leaks of negotiating texts and official statements of negotiating objectives shed some light on their likely content.[16] This section will look at the issue of cross-border information flows in three major ongoing trade negotiations: the Trade in Services Agreement (TISA), the Trans-Pacific Partnership (TPP), and the Transatlantic Trade and Investment Partnership (TTIP).

TRADE IN SERVICES AGREEMENT (TISA)

The TISA is a plurilateral agreement being negotiated between 24 parties, including the EU, the US, and a diverse group of countries, such as Pakistan, Panama, South Korea, and Turkey.[17] TISA negotiating parties represent nearly 1.6 billion people and a combined GDP that is nearly two-thirds of the world's economy.[18] TISA seeks to build on the language of the GATS and further liberalise service sectors, including telecommunication, delivery, and technology.[19] In July 2015, Wikileaks published a set of documents from the TISA negotiations.[20]

The Annex on Electronic Commerce includes a proposal from Canada, Colombia, Japan, Taiwan, and the US that would strongly discourage data localisation mandates. The proposal would prohibit parties from blocking cross-border information transfers, including personal information when the activity is carried out in connection with the service supplier's business.[21] Colombia and the US further propose language that would bar local infrastructure requirements for cross-border information service providers.[22] Japan similarly proposes that no state be permitted to require information service suppliers to establish a local presence as a condition to supply services. Such TISA obligations would bar efforts to force information service providers to locate data servers within particular countries, subject to exceptions for national security and conservation of living and natural resources.[23]

The free flow of information obligations set forth in the Electronic Commerce chapter are still subject to negotiation and possible narrowing. For example, South Korea has proposed that movement of information across borders must be based on "informed consent," with full protection and recourse under the law in regards to use of personal information.[24] We return to the issue of consent in the final section below.

15 Lovejoy, Katherine A. "A Busted Flush: Regulation of Online Gambling in the European Union," 37 *Fordham Int'l L.J.* 1525, 2014.

16 De Pillis, Lydia. "The catch-22 of trade deals done in secret," *Washington Post*, May 15, 2015.

17 European Commission, Trade in Services Agreement http://ec.europa.eu/trade/policy/in-focus/tisa/

18 Government of Canada, Trade in Services Agreement http://www.international.gc.ca/trade-agreements-accords-commerciaux/topics-domaines/services/tisa-acs.aspx?lang=eng

19 Office of the United States Trade Representative, Trade in Services Agreement https://ustr.gov/TiSA#

20 Dayen, David. "The Scariest Trade Deal Nobody's Talking about just Suffered a Big Leak," *New Republic* (July 4, 2015); Wikileaks, July TISA Release https://wikileaks.org/tisa/.

21 TISA Annex on Electronic Commerce https://wikileaks.org/tisa/ecommerce/05-2015/page-3.html

22 Id. at pg.8 https://wikileaks.org/tisa/ecommerce/05-2015/page-8.html

23 On the national security exceptions to the WTO agreements, see Abdel-Latif, Ahmed. How to deal with the security exception in the digital economy, E15 Initiative paper (2015)

24 Id.

TRANS-PACIFIC PARTNERSHIP (TPP)

Another diverse group of countries has concluded negotiating a text for the TPP. The 12-country partnership among a group of Pacific nations from Australia to Vietnam covers a zone with 39 percent of the world's GDP.[25] The subjects of the negotiations are quite broad, dealing with cross-cutting issues, including agriculture, customs, and electronic commerce.[26]

If enacted, the TPP will include some of the strongest general commitments to the free flow of data in the world trade system. TPP member states make two broad commitments in this area: first, to permit the cross-border transfer of information, and second, to not impose regulations that require companies from TPP member states to use local computer servers. Specifically, Article 14.11 mandates that member states must allow the cross-border transfer of data. However, the TPP permits restrictions on that transfer if the restrictions are (1) designed to achieve a legitimate public policy objective; (2) not applied in a manner that constitutes unjustifiable discrimination; and (3) not greater than those required to achieve the objective. The provisions do not apply to the information that TPP member governments themselves collect or, relatedly, to government procurement.[27]

In sum, legitimate public policy objectives such as privacy can limit cross-border flow of data or require the use of a local computing infrastructure, as long as they meet the criteria specified above. But if protection of consumer or business privacy can be achieved consistently with international data flows, then such flows should be allowed. This lends support to the U.S. government's characterization of the TPP as "the most ambitious trade policy ever designed for the Internet and electronic commerce."[28]

THE TRANSATLANTIC TRADE AND INVESTMENT PARTNERSHIP (TTIP)

The TTIP represents an effort to create a liberal trade zone across the Atlantic between the US and the EU.[29] The agreement would cover one-third of global goods and services trade as well as nearly half of global economic output.[30] Also, like the TPP, the negotiation covers a wide array of subjects.[31]

While the negotiations have been conducted largely in secret, the British Broadcasting Corporation (BBC) released a document described as the EU's "initial offer" in the negotiations with respect to the schedule of commitments, but excluding its offers with respect to modes 1 and 2 (cross-border trade in services and consumption abroad).[32]

It is quite likely that the US proposal on data flows will be similar to the one it proposed in both TISA and the TPP, both because of the strategic importance of information flows and the inherent usefulness of harmonised trade agreements. The EU has stated that it believes that its data protection laws will not be affected by the TTIP, but the issue remains a focus of the discussions. In March 2015, Juhan Lepassar, head of EU Digital Commissioner Andrus Ansip's cabinet, stated that the EU is on the same page as the US on information flows and the issue could be considered in the TTIP negotiations.[33]

The European Parliament has recommended that the cross-border flows of data provisions in the TTIP should be consistent with existing EU privacy law.[34] We turn now to the question of whether the free flow of data across borders is indeed compatible with privacy and security.

25 United States Trade Representative, The Trans-Pacific Partnership: Economic Benefits, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2013/December/TPP-Economic-Benefits.

26 Stoller, Matt. Trans-Pacific Partnership: The biggest trade deal you've never heard of, Oct. 23, 2012.

27 TPP Art. 14.2.

28 https://medium.com/the-trans-pacific-partnership/electronic-commerce-87766c98a068; David Fidler, The TPP's Electronic Commerce Chapter: Strategic, Political, and Legal Implications, Council on Foreign Relations Blog, Nov. 9, 2015, http://blogs.cfr.org/cyber/2015/11/09/the-tpps-electronic-commerce-chapter-strategic-political-and-legal-implications/.

29 Office of the United States Trade Representative, Transatlantic Trade and Investment Partnership https://ustr.gov/ttip

30 Office of the United States Trade Representative, Fact Sheet: United States to Negotiate Transatlantic Trade and Investment Partnership with the European Union https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2013/february/US-EU-TTIP

31 Directorate-General for Trade of the European Commission, http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153635.pdf.

32 Campbell, Glenn. "TTIP: Transatlantic trade deal text leaked to BBC," BBC News, Feb. 2015. http://www.bbc.com/news/uk-scotland-scotland-politics-31631461

33 Fleming, Jeremy. "Brussels makes overture on 'data flow' agreement in TTIP," EurActiv.com, Mar. 30, 2015.

34 European Parliament, Resolution of 8 July 2015 containing the European Parliament's recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI)): to ensure that the EU's acquis on data privacy is not compromised through the liberalisation of data flows, in particular in the area of e-commerce and financial services, while recognizing the relevance of data flows as a backbone of transatlantic trade and the digital economy; to incorporate, as a key point, a comprehensive and unambiguous horizontal self-standing provision, based on Article XIV of the General Agreement on Trade in services (GATS), that fully exempts the existing and future EU legal framework for the protection of personal data from the agreement without any condition that it must be consistent with other parts of the TTIP; to negotiate provisions which touch upon the flow of personal data only if the full application of data protection rules on both sides of the Atlantic is guaranteed and respected to cooperate with the United States in order to encourage third countries to adopt similar high data protection standards around the world…

PROTECTING PRIVACY AND SECURITY

Critics of cross-border information flows argue that such flows jeopardise privacy and national security. We suggest that privacy and national security can be protected in international trade agreements if they are properly structured. We go further to argue that international flows can even strengthen privacy and national security, while avoiding the economic losses that result from cutting off foreign suppliers of goods or services.[35]

We begin by observing that international trade law has long dealt with concerns about consumer protection in a world of liberalised trade. Take the case of what is perhaps the most important product area related to consumer protection—food. Each member of the WTO crafts its own food safety standards, and imposes those standards on the food it imports. The WTO's Sanitary and Phytosanitary (SPS) Measures Agreement affirms nations' right to set their own food safety standards[36] Food safety standards, however, cannot be arbitrary. Rather, they must be based on science, so that they are not used as a disguise for protectionism.[37] The SPS Agreement also encourages nations to agree on international standards, guidelines, and recommendations, although again it permits nations to establish higher health standards as long as they are based on science.[38] The food safety standards demonstrate that even when international trade law applies, "foreign products can be denied market access, unless they meet the established requirements."[39] The ultimate result is this: consumers have access to food from around the world, while governments can still restrict unsafe foreign or domestic foods.

Similarly, can we allow global information flows and still protect public order, privacy, and security? It is important to note that the TISA E-commerce chapter draft does not ban national public order, privacy, and security rules. Rather, the draft rules target government regulations that require foreign service providers to keep information within the country. The draft rules provide that no country can require a foreign service supplier to, "store or process data in its territory."[40] Relatedly, a member state could no longer prevent a foreign service supplier from transferring information outside that member state. Thus, the TISA or the TPP would interfere with privacy rules, for example, only to the extent that they require that information stay within a country.

The question then is whether rules that bar information from being placed outside the country advance the privacy and security of that country's citizens. Like money stored under the mattress, information is not necessarily more secure if it is kept at home. Criminals may gain illicit access even if the information is stored within the individual's home country. After all, criminal hackers do not stop at national borders. Indeed, data localisation obligations reduce the choice of information providers available to consumers and businesses. As a recent cover feature of the *IEEE Computer Society* magazine observes, "The most common threats to data in the cloud involve breaches by hackers against inadequately protected systems, user carelessness or lack of caution, and engineering errors."[41] Thus, prohibitions on data localisation increase access to service providers from around the world, allowing individuals and businesses to choose service providers with the best privacy and security practices.

Furthermore, countries can still insist that their public order, privacy, and security requirements be followed by foreign providers wherever they store or process data. This is a common practice in cross-border outsourcing arrangements, where the outsourcing provider commits to protect information consistent with local standards. Indeed, permitting cross-border flows is likely to enhance privacy and security as it allows consumers and businesses to select from a wider range of providers that are subject to global competition.

One approach has been to require a person's consent before his or her personal information can be transmitted across borders. But, this approach is likely to prove a major impediment to many kinds of information flow. We do not typically require a special consent before a consumer purchases a good, or even food, from a foreign source. There are reasons to believe that a consent requirement for information transfer will prove difficult to satisfy, and thus itself function effectively as a barrier to cross-border flows of information. It may be difficult to know, for example, whether consent has been meaningfully obtained, as companies simply add "cross-border data transfer" to their lengthy list of terms and conditions. Imagine the difficulties of obtaining such consent when it comes to devices that capture information about more than one person. Many

35 For an important discussion of the application of the General Agreement on Trade in Services to national privacy standards, see Weber, Rolf H., Regulatory Autonomy and Privacy Standards. Under the GATS, Asian Journal of WTO & International Health Law and Policy, Vol. 7, No. 1, pp. 25-48, March 2012.

36 Agreement on the Application of Sanitary and Phytosanitary Measures (SPS Agreement), Art. 2.1.

37 SPS Agreement, Art. 2.2.

38 SPS Agreement, Arts. 3.1 & 3.3.

39 Mavroidis, Petros C. Trade in Goods 709. 2d ed., Oxford 2012.

40 TISA Draft, Art. 9, https://wikileaks.org/tisa/ecommerce/05-2015/page-8.html.

41 Ryan, Patrick S., Sarah Falvey, and Ronak Merchant, "When the Cloud Goes Local: The Global Problem with Data Localization," *COMPUTER*, Dec. 2013, at 54, 56.

applications will involve personal data not only of the contracting counterparty, but also of third parties. An email, for example, might include personal information not only about the person receiving the message, but also about others, as might a device that monitors a particular environment. Will a self-driving car need the consent of every other inhabitant of a vehicle it encounters if the self-driving car processes information about road conditions remotely?

Finally, both the TPP released text and the TISA draft proposal include language that would oblige member states to adopt consumer protection laws and promote cooperation among national consumer protection agencies.[42] Both texts also require each member state to provide a legal framework to protect personal information.[43] Ultimately, the protection of privacy and security online will turn not on counterproductive and mostly futile bars against cross-border information flows, but on both international cooperation between states and international competition between suppliers.

On the issue of public order, trade policy could adopt a model used for aspects of Internet governance, namely the multi-stakeholder process with publication of best practices.[44] Such a process could help governments understand similarities and divergences in the treatment of content on the Internet. Governments could share tactics on how to effectively target and combat content that is considered a threat to public order, while avoiding unilateral executive branch censorship determinations likely to violate the freedom of expression. For example, the positives and negatives of proposals for data localisation, domain name takedowns, or filters could be discussed in an open forum before domestic actions are taken. Such a discussion would not create binding commitments, but rather improve the sharing of information, including best practices. Such informal discussions could greatly improve outcomes for governments in their efforts to support domestic public order concerns, and might reduce actions that would harm the open-interconnected network that is the Internet.

While privacy laws across the world will likely continue to differ, there are several related principles that are shared across regions. The importance of dignity, free association, and the security of personal data are universally recognised. These ideas can and should be included as part of trade discussions about the free flow of information. Even if trade policy cannot achieve harmonisation on privacy rules, it can promote the interoperability of different privacy rules. The existing US-EU Safe Harbor enables US businesses that would not otherwise qualify under the EU's data protection directive to meet some of the important goals of the EU framework, subject to enforcement by the Federal Trade Commission.[45] This system thus operates to create interoperability between two otherwise different systems.

CONCLUSION

Cross-border information flows underlie nearly every aspect of the modern economy. Governments are legitimately concerned with ensuring that cross-border information flows support public order, national security, and consumer privacy. Trade policy has only begun to address this issue in the past few years, and there has to date been binding language on the topic. We argue that specific binding trade language on cross-border information flows — combined with continued international cooperation — will enhance, not undermine, public order, national security, and privacy.

42 TPP, Art. 14.7; TISA Draft, Art. 3.

43 TPP, Art. 14.8; TISA Draft, Art. 4(2).

44 Waz, Joe and Phil Weiser. " Internet Governance: The Role of Multistakeholder Organizations," 10 *J. on Telecomm & High Tech L.* 331, 338, 2013.

45 Mcbride, Naomi, Lisa J. Sotto, and Bridget Treacy, Privacy & Data Security: The Future of the US-EU Safe Harbor, Hunton Privacy Blog, 2013. Available at: https://www.huntonprivacyblog.com/files/2013/12/Privacy-Data-Security-The-Future-of-the-US-EU-Safe-Harbor.pdf

ADDITIONAL REFERENCES

Makiyama, Hosuk Lee. "Digital Trade in the U.S. and Global Economies," *European Centre for International Political Economy*, accessed February 10, 2015, http://www.ecipe.org/app/uploads/2014/12/USITC_speech.pdf.

Kuner, Christopher. Transborder Data Flow Regulation and Data Privacy Law. Oxford, 2013.

Pélissié du Rausas, Matthieu. et al., "Internet matters: The Net's sweeping impact on growth, jobs, and prosperity," *McKinsey Global Institute,* May 2011, http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

Castro, Daniel andMcQuinn, Alan. Cross-Border Data Flows Enable Growth in All Industries, Feb. 2015, http://www2.itif.org/2015-cross-border-data-flows.pdf.

Meltzer, Joshua. "The Internet, Cross-Border Data Flows and International Trade," *Asia & the Pacific Policy Studies*, vol. 2, no. 1, pp. 90–102.

Chander, Anupam. The Electronic Silk Road: How the Web Binds the World Together in Commerce. Yale, 2013.

Implemented jointly by ICTSD and the World Economic Forum, the E15Initiative convenes world-class experts and institutions to generate strategic analysis and recommendations for government, business, and civil society geared towards strengthening the global trade and investment system for sustainable development.

ICTSD
International Centre for Trade and Sustainable Development

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD