No Trade Off:

How the Free Flow of Data Enhances Trade and Human Rights

IHRB

Institute for Human Rights and Business

Institute for Human Rights and Business
Postal address: 34b York Way,
London, N1 9AB, UK
Phone: (+44) 203-411-433
Email: info@ihrb.org
Web: www.ihrb.org

Cite as: Institute for Human Rights and Business (IHRB), "No Trade Off: How Free Flow of Data Enhances Trade and Human Rights" (July 2016).

Acknowledgments: Anita Ramasastry, Professor of Law at the School of Law at the University of Washington Law School, and IHRB Senior Research Fellow, Lucy Purdon, IHRB ICT Project Manager, and Salil Tripathi, IHRB Senior Advisor for Global Issues, co-authored this report, with advice from Motoko Aizawa, IHRB Managing Director USA.

IHRB wishes to thank the Ministry of Foreign Affairs of Sweden for its financial support for this Report.

See: http://www.ihrb.org/focus-areas/information-communication-technology/ for more information about IHRB's work in the area of information and communications technology (ICT) and human rights.

Contents

Acronyms

CJEU	Court of Justice for the European Union
GATT	General Agreement on Tariffs and Trade
GCHQ	Government Communications Headquarters (of the United Kingdom)
FTC	Federal Trade Commission (of the United States)
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social, and Cultural Rights
ICT	Information and Communication Technology
ISP	Independent Service Provider
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
NSA	National Security Agency (of the United States)
OECD	Organisation of Economic Cooperation and Development
OAS	Organization of American States
SDGs	Sustainable Development Goals
SMEs	Small and Medium-Sized Enterprises
TiSA	Trade in Services Agreement
TPP	Trans-Pacific Partnership
T-TIP	Transatlantic Trade and Investment Partnership
VoIP	Voice over Internet Protocol
WTO	World Trade Organization

Executive Summary

Cross border data flows are integral to international trade transactions, which increasingly rely on information exchange, electronic payments, and cloud storage. These movements often involve the analysis of large amounts of personal information, otherwise known as "big data".[1] The free flow of data - which in the context of trade refers to cross border economic activity unrestricted by tariffs or non-tariff barriers - raises a number of national and international security issues. For example, the implications of large amounts of personal information in public or private hands, at times in a single location, has only recently become a subject of broader debate, raising legitimate concern among governments and citizens alike. What companies or government agencies do with the data they collect and store is another critical issue. If personal data is misused or accessed without authorisation, it may lead to adverse impacts on protection of internationally recognised human rights.

Issues relating to the movement and collection of data have gained greater prominence in recent years, following revelations that the National Security Agency (NSA) in the United States, the Government Communications Headquarters (GCHQ) in the United Kingdom, and other intelligence agencies worldwide had engaged in mass collection and sharing of phone and Internet data, otherwise known as "communications data" or "metadata".[2] This controversy raised fresh questions concerning:

- The relationship between governments and businesses in the context of data gathering and sharing;
- The extent of intrusive surveillance by governments with or without the knowledge of companies and consumers and actions taken as a result that may adversely impact human rights standards; and
- The decisions Information and Communication Technology (ICT) companies face with respect to data shared with governments.

These developments have dominated on-going discussions concerning the human rights responsibilities of the ICT sector, the impact on cross-border data flows, and further highlight the need to address surveillance issues in countries around the world. Allegations of mass surveillance by governments and related concerns that data flows are restricted in some countries to avoid surveillance by other governments, and the responsibilities of ICT companies in these situations, have been identified as critical challenges requiring constructive discussion and joint action.

It is clearly important to ensure that state reactions to mass surveillance allegations do not lead to measures that restrict the free flow of information generally. Undue state restrictions on data flows risk stifling local innovation and may prevent domestic businesses from accessing new opportunities and markets through the use of technology. Access to data is vital to individuals and businesses both in fostering economic opportunity and in promoting greater respect for human rights.

The Trade Policy Department at the Ministry of Foreign Affairs in Sweden approached IHRB to apply learning from the Digital Dangers project to the issue of how restrictions on the free flow

1 See a further explanation of "big data" here from UK NGO Privacy International

2 See a further explanation of "metadata" here from Privacy International

of data could not only negatively affect trade worldwide but also adversely impact respect for international human rights standards. This report builds on earlier studies by the Swedish National Board of Trade - "No Transfer, No Trade"[3] and "No Transfer, No Production".[4] Both of these reports outline the importance of cross-border data transfers for companies based in Sweden. An earlier IHRB discussion paper (also entitled "No Trade Off")[5] provided input for a session at the Stockholm Internet Forum in May 2014. The discussion paper focused on the importance of reconciling privacy and security concerns as part of efforts to promote economic development.[6] That discussion prompted further research, including visits by IHRB staff members to Myanmar and Brazil, which complemented a previous visit to Kenya, all focused on challenges facing the ICT sector.

With support from the Swedish Ministry for Foreign Affairs, in 2014 IHRB organised a high-level event at Wilton Park titled *Privacy, Security and Surveillance: Tackling Dilemmas and Dangers in the Digital Realm*[7], which brought together 60 business, government and civil society stakeholders from 18 countries to discuss ways to ensure safety and security while protecting privacy in the digital realm, particularly with regard to state responses to threats and dangers.

This report draws on the previous work referenced above and examines six areas in which government-imposed restrictions on the free flow of information could impact negatively on trade and human rights.

- **Data localisation/storage requirements**: Users and businesses may be able to choose where their data is stored, which may lower costs for businesses and grant users greater autonomy over their personal information, aligning data more squarely with ownership. However, some States are forcing companies to store data on servers within their jurisdiction, thus raising concerns about who can access the data and under what circumstances.

- **Encryption:** Security of user data, authentication and confidentiality are critical in building consumer trust in e-commerce. Security of information through encryption is not just important for safe transactions - it is also important for human rights defenders, journalists, minorities, and others at risk, who fear confidential communications may be intercepted arbitrarily by intelligence agencies.

- **Content censorship through filtering/blocking:** State efforts to censor online content have potentially serious consequences for protecting freedom of expression. Although the human rights impacts of such actions are widely discussed, the economic and trade implications of online censorship have received far less attention.

- **User registration requirements:** State imposed registration requirements for mobile phones and SIM cards enable governments to track user locations and movements, potentially endangering personal security, safety, and privacy. Moreover, mandatory

3 Kommerskollegium, The National Board of Trade, No Transfer, No Trade- The Importance of Cross-Border Data Transfers for Companies Based in Sweden. (2014)

4 Kommerskollegium, The National Board of Trade No Transfer, No Production- A Report on Cross-Border Data Transfers, Global Value Chains, and the Production of Goods. (2015)

5 IHRB (2014) Discussion Paper: No Trade Off. Restrictions on the Free Flow of Data, World Trade and Human Rights

6 Stockholm Internet Forum 2014, No Trade Off panel summary and video.

7 Wilton Park conference report (2014)

registration places costs on operators, and could depress growth in mobile penetration, potentially affecting livelihoods and acting as a barrier to widening the range of SIM distribution channels.

- **Connectivity and Access:** Accessible and affordable Internet connections are critical to economic and social development. Digital communication is an enabler of important human services, such as accessing health information, mobile banking and emergency services. Users, including companies, are able to make use of cloud computing and new sources of credit and financing, only by relying on Internet access. State imposed mobile and Internet network shutdowns risk adverse impacts on the enjoyment of human rights. They also undermine economic development, as companies may not see the benefit in investing in more efficient technical management systems if they are subject to regular shutdowns that block access to the Internet.

- **Restrictions on cross border data flows:** As of 2013, 99 countries have adopted some form of data protection and privacy legislation that restricts the use and transfer of personal or other sensitive data.[8] This form of regulation is primarily intended to protect individuals' right to information, privacy, and to prevent the misuse of personal information. While sound in intent, such laws can become restrictive, and may disrupt commerce because legal frameworks across countries differ, creating compliance costs and increasing unpredictability for firms.

The following sections provide an overview of the connections between trade and human rights and the importance of data flows in this context, as well as current threats and obstacles to cross border trade and the free flow of information. It is evident that governments should refrain from restricting flow of data including cross border flows, unless there are legitimate public policy concerns that are clear to the public, based on transparent and specific criteria, which allow for the public and others to understand the rationale for such restrictions. Policy makers should develop strategies and methodologies to determine and quantify how restrictions on cross border data flows impact trade, market access, economic and social development, as well as affect the realisation of certain human rights through digital access. In parallel with consideration and creation of such strategies and methodologies, governments should improve transparency and predictability in their actions on restrictions of data flow, and on regulation of the digital economy generally, in consultation with civil society organisations as well as relevant companies in the ICT sector and beyond.

The interplay of trade and human rights has been scrutinised extensively in terms of rules that should be established as a common baseline. The debate is not whether trade should take place, but whether differential rules should be permitted for countries at various stages of economic development. This report does not address the larger debates over the merits of particular trade rules. Instead it explores the finer point that freer information flows benefit businesses at all stages of development and within global value chains, and furthermore, that restrictions against free flow of information often create human rights harms.

8 Graham Greenleaf, Local Data Privacy Laws 2013: 99 Countries and Counting Privacy Laws & Business International Report, Issue 123 (June 2013) pp. 10-13

I. Understanding Links Between Trade, Human Rights and Data

Trade is of critical importance to expanding economic opportunities for people across the globe. Trade brings economic benefits and contributes to the realisation of human rights. But trade without rules, without principles, without laws or regulation, can also undermine human rights protections.

The underlying principle of the World Trade Organisation (WTO) is to promote more trade and to remove restrictions based on the theory that greater trade increases economic growth and development. The principles include trading without discrimination among and between nations under the most-favoured-nation treatment (that means countries must treat all member states equally, and cannot offer preferential terms to some states over others); treating foreign and local firms equally; expanding trade through negotiations; agreeing to binding agreements and transparently; and promoting fair competition.

Exceptions are permitted under strict conditions in cases where countries have set up a free trade agreement that applies only to goods traded within themselves (and therefore discriminating against goods from outside, by forming regional blocs, such as the North American Free Trade Area or the European Union); or by granting preferential or special access to developing countries to their markets; or by raising trade barriers such as duties against products that are being traded unfairly from certain countries; or in certain specific services.

WTO agreements permit exceptions to liberalising trade under specific conditions, such as protection of public health and the environment.[9] Likewise, other treaties, such as in the area of investment, often include clauses that allow states to intervene temporarily and impose standards to protect public health and other criteria consistent with those found in WTO agreements.

Most nations have signed and ratified international conventions (in particular the core conventions of the International Labour Organisation[10]) that set standards for labour rights. Furthermore, many countries have given the conventions legal effect by enacting enabling legislation as part of their domestic laws. Trade liberalisation should not mean undermining those standards. Activist groups rightly focus on labour rights abuses that occur in global supply chains, including child labour, sexual harassment and abuse, violence against the vulnerable, and other exploitative conditions. While trade without restrictions can have adverse consequences for human rights, such as loss of jobs in industries that cannot compete with

9 Article 20 of the GATT states that provided a restriction being imposed is justified, not arbitrary, and nor a disguised restriction on trade, a country can impose restrictions if a specific trade of goods or service violates certain basic conditions. These include protecting public morals, protecting human, animal or plant life, trading gold and silver, to comply with laws that are consistent with the multilateral trading arrangement, related to products from prison labour, protecting cultural or artistic heritage, conserving exhaustible natural resources, complying with other commodity trade agreements, to meet specific shortages, and to comply with an economic stabilisation plan.

10 The ILO core conventions. These are: 29 (Forced Labour) of 1930; 87 (Freedom of Association and Protection of the Right to Organise) of 1948; 98 (Right to Organise and Collective Bargaining) of 1949; 100 (Equal Remuneration) of 1951; 105 (Abolition of Forced Labour) of 1957; 111 (Discrimination – Employment and Occupation) of 1958; 138 (Minimum Age Convention) of 1973; and 182 (Elimination of the Worst Forms of Child Labour) of 1999 ctf.

imports, there can be similar adverse consequences when restrictions are imposed on trade in the name of human rights. For example, restrictions placed ostensibly for human rights or environmental protection may lead to a ban on imports, which may be cheaper, and may increase the price of products in a home market, affecting the poor. This may be more apparent when the trade is in tangible commodities, but is as true when transactions involve digital goods and services. Laws restricting trade are consistent with human rights standards only where the restrictions are designed and implemented to protect the vulnerable from harm.

In the case of the flow of data, restrictions can have detrimental impacts on trade, industries, and especially small and medium sized enterprises (SMEs), as well as on human rights, including the right to seek, receive and impart information; the right to health; the right to education; the right to participate in political processes; the right to demonstrate peacefully; the right to a decent livelihood; and the right to life itself.

Currently, two major trade agreements are under discussion: the T-TIP (the Transatlantic Trade and Investment Partnership) is a potential agreement between the United States and the European Union; and some fifty members of the WTO, including EU member states are negotiating the Trade in Services Agreement (TiSA). In October 2015, a group of twelve Pacific Rim nations concluded negotiations on the Trans-Pacific Partnership (TTP), billed as a 21st century trade agreement, which includes provisions focused on the "free" flow of data.

While governments are negotiating to allow for greater movement of information in the trade context, the mass surveillance revelations of 2013 damaged trust between governments and citizens, governments and business, business and their users and between governments themselves. This mistrust contributed to measures to control the flow of data beyond borders. In 2015, the Court of Justice for the European Union (CJEU) invalidated the "Safe Harbour" agreement between the United States (US) and the European Union (EU), which allowed for data transfer from the EU to the US. The Court ruled that European citizens' privacy was compromised, as personal data stored by companies in the US was not adequately protected from US government surveillance. According to the CJEU, this constituted a violation of EU data protection rules. While a victory for privacy advocates, it has implications for business reliant on the transatlantic transfer of data. For additional analysis of the CJEU case, see Annex 2.

In recent years, governments have deployed several legislative and regulatory measures aimed at prohibiting the use of certain technologies or applications, blocking website content, and requiring that data reside on local servers all as a means of controlling and impeding information flows. These restrictions are imposed, at times, with a view to protecting national security or national interests. Such restrictions may curb privacy as well as other human rights, and may limit legitimate economic activity, including cross border trade. At other times, governments may take actions that restrict data flows, using the argument of protecting national security or other strategic interests, when in fact their real purpose may be to create disguised trade barriers.

Trade Barriers, the Internet, and Human Rights

The Internet disrupts old economic models. For example, companies that sell music, books, or access to films through the Internet destabilise existing markets and retail trade, but offer a service existing retail trade is often unable to provide. Market aggregators that enable buyers and sellers to meet directly are eliminating middlemen and lowering transaction costs, including for consumers.

The Internet allows, for example, peer-to-peer platforms, where smaller businesses and consumers can seek access to credit, offer services and exchange goods directly.[11] In the new sharing economy, individuals can become entrepreneurs – letting their apartments to tourists directly, for example.

In response to such disruption and new business models, governments have sometimes considered imposing restrictions on new technologies or Internet usage. Restrictions imposed on trade through the Internet are another way of protecting domestic business or practices. These restrictive steps by governments may not always serve a legitimate public purpose. They do, however, support existing monopolies, and thereby can increase costs for consumers.

But more than that, they may also undermine respect for human rights. What Internet-based companies do is to trade on information. Buyers and sellers get access to prices of cheaper products and services through the Internet; restricting access to such data prevents them from securing the best deal. This could be seen as infringing on the right to information. Restricting the Internet by cutting off access to online services ostensibly to protect society against terrorism or other threats may hurt small businesses reliant on international markets. It could also prevent doctors at primary health care clinics seeking access to a service such as Skype to speak at no cost to doctors overseas; prevent farmers from selling commodities into global value chains; hinder students who need to access digital libraries; stop journalists or human rights defenders from disseminating their work, and make it more difficult for people seeking to participate in political protests to communicate with one another.[12]

11 Sundararajan, Arun. "Peer-to-Peer Businesses and the Sharing (Collaborative) Economy: Overview, Economic Effects and Regulatory Issues." Written testimony for the hearing titled 'The Power of Connection: Peer-to-Peer Businesses' at the United States House of Representatives (2014). "The platforms are the person-to-person marketplaces which facilitate the exchange of goods and services between peers. The entrepreneurs are the individuals or small businesses that supply goods and services in these marketplaces. The consumers are the individuals who demand: buy, rent, consume. (Both the entrepreneurs and the consumers are often referred to as 'peers'.) Typically, the payment from the consumer to the entrepreneur is mediated by the platform, which often charges a commission to one or the other trading party. For example, in the context of peer-to-peer accommodation: Airbnb and VRBO are platforms, an individual who offers living space for short-term rentals is the entrepreneur, and an individual who rents the living space from the entrepreneur is the consumer."

12 See also IHRB, Security v Access: The impact of mobile network shutdowns. Case study: Telenor Pakistan (2015)

Implications for Trade and Economic Development

The Internet is no longer only a digital storefront. It is a dynamic platform that increases productivity and the ability of businesses to compete. Understanding the Internet as a platform for trade highlights its broad economic potential. Commercial opportunities are no longer limited to Internet companies, but are now available for businesses in all sectors of the economy, from manufacturing to services.

According to the International Telecommunications Union (ITU), over 3 billion people are Internet users and there are more than 7 billion mobile phone subscriptions worldwide.[13] Every industry is undergoing rapid digital transformation. Even traditional industries, such as manufacturing and agriculture, which will always see movement of physical goods, also increasingly rely on technology and the movement of data to conduct business. Manufacturers, retailers, and farmers alike, depend on the transfer of data to participate in global supply and value chains.[14]

The Swedish National Board of Trade report, "No Transfer, No Production" outlines five main reasons why manufacturers need to move data:[15]

- To control and co-ordinate geographic production in parallel.
- To conduct research and development (R&D) in the pre-production phase.
- To ensure efficient supply chain management.
- To manage production processes.
- To monitor goods in the post-sale phase.

The McKinsey Global Institute estimates that the Internet alone accounted for 21% of aggregate growth in gross domestic product (GDP) across thirteen of the world's largest economies from 2006 to 2011, with 10% of that growth occurring for SMEs.[16] There have been some attempts to quantify the Internet's impact on growth and international trade. For example, a study of OECD countries from 1996-2007 finds that a 10% increase in broadband penetration (during the first decade of broadband diffusion) raised annual per capita growth by 0.9-1.5%.

A study using data from 1996-2011 finds similar results: a 10% increase in broadband penetration is correlated with a 1.35% increase in GDP for developing countries and a 1.19% increase for developed countries.[17] The World Bank also reports that the ICT sector accounts for

13 ITU, The World in 2015: ICT Facts and Figures

14 Smith, Gail and Martindale, Wayne, Food supply chains-our current understanding, Aspects of Applied Biology 102 (2010): 75-80; World Economic Forum, Outlook on the Logistics and Supply Chain Industry (2013); Global Commerce Initiative, The Future Value Chain (2006).

15 Kommerskollegium, The National Board of Trade, No Transfer, No Production- A Report on Cross-Border Data Transfers, Global Value Chains, and the Production of Goods (2015), p9

16 Ibid

17 Joshua Meltzer, Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium-Sized Enterprises and Developing Countries, Brookings Institution (Global Economy and Development Working Paper 69, February 2014)

one-quarter of GDP growth in developing countries.[18] In India, the growth of mobile applications and mobile commerce has created an estimated 7 million jobs.[19]

However, these developments rely on Internet access, which is lacking or is in short supply in many developing countries. The costs of connectivity are often prohibitive and connections frequently unreliable. As McKinsey reports:

> *'Despite the promise of the Internet as an equalising platform, the growing digital divide could leave developing economies further behind."*[20]

Access to the Internet is increasingly critical for businesses large and small. Many rely on the cloud to store various types of data including traditional back-office functions. Human resources, payroll, customer relationship management data, accounting, finance, project management and application development are often stored in the cloud. This data needs to be accessible to businesses and often needs to move across borders to different company locations, or to customers or clients in various geographies. Placing restrictions on such data increases transaction costs and causes delays.[21]

As companies and individuals are transmitting more information online, and storing it in the cloud, some governments are seeking to impose limits on the free flow of information. Governmental limitations on the free flow of information are a clear threat to open markets and trade. Countries with higher openness on the Internet as measured by the Freedom on the Net Index[22] also have better scores on the Economic Impacts Pillar of the World Economic Forum's Networked Readiness Index. A 2014 report by Dalberg Development Advisors[23] concluded that a country with fewer restrictions (categorized as "free" by the Freedom on the Net index) is more likely to have a more robust Internet economy when we account for GDP per capita. Similarly, countries with more restrictions (categorised as "partly free" or "not free") are more likely to be worse off in terms of the strength of their Internet economy even when we correct for GDP per capita.

Regulatory barriers restricting market access to ICT companies can limit the growth of Internet access and prevent the widespread adoption of the Internet as a business tool. A recent comparison between approaches to broadband in Kenya and Senegal illustrates this effect. While proactive policymaking on broadband in Kenya has been critical to expanding affordable access, in Senegal, regulations have made it difficult for broadband operators to obtain licenses, limiting the number of service providers and creating a de facto monopoly. Users have few options to choose from, and prices remain high. While Kenya and Senegal had similar levels of Internet penetration in 2005 — and Senegal's growth even outpaced Kenya's in certain years — Kenya quickly leapt ahead following the liberalisation of markets. In 2012, Senegal's Internet penetration remained below 20%, while Kenya's had grown to 32%.[24] By the end of 2015, Internet penetration in Senegal was 52% while Kenya's was 70%.[25]

18 World Bank, Information and Communications for Development 2009: Extending Reach and Increasing Impact

19 Joshua Meltzer, Supporting the Internet as a Platform for International Trade, supra note 23

20 McKinsey Global Institute Global Flows in a Digital Age: How Trade, Finance, People and Data Connect the World Economy (2014) p15

21 Karl Mivilee de Chenem Practicing International Trade at pp. 24-26 (2014)

22 Freedom House, Freedom on the Net Index (2015)

23 Dalberg Development Advisors, Open For Business, The Economic Impact of Internet Openness (2014)

24 Ibid at 34

25 Internet World Stats, Africa (2015)

Implications for SMEs

Online platforms now allow even the smallest business or sole proprietor to reach a global customer base. According to a 2014 McKinsey Global Institute report[26], 90% of traders on eBay export to other countries, compared with less than 25% of traditional small businesses.[27] In addition, data is a commodity in itself, in the form of e-books, music, films and games bought, sold and stored on an increasing number of devices such as e-readers, MP3 players and games consoles. The development of 3-D printing means that the template of a physical object can be transferred online via a digital file and physically produced in another location.
By enabling the transfer of data, the Internet offers three main benefits for SMEs:

- **Lower Transaction Costs.** The Internet facilitates buying and selling, consumer feedback, market and product research, and marketing. E-commerce applications reduce costs associated with making payments, customer service, product display, inventory management, and even staff recruitment.

- **Wider Reach.** Small businesses easily become global businesses via the Internet. SMEs can enter distant markets and target more customers, creating new channels for revenue generation. Social media enables inexpensive marketing as satisfied customers promote SMEs among their friends. With an expanded customer base, both domestically and internationally, these "micro-multinationals" can enjoy more revenue, profit, and productivity.

- **More Knowledge.** The Internet can improve SMEs' awareness of competitors and input costs, thus making innovation less costly in terms of time and money. It can also increase SMEs' knowledge of government initiatives and policies that support SMEs.

According to a 2012 study focused on eBay, SMEs using the Internet for 12 years have 21% higher revenue, 25% higher profit, 37% higher employment, 35% higher employment growth, and 9% customer growth as compared to an SME that has been using the Internet for only six years.[28] A 2013 study in Australia shows that small businesses using the Internet extensively in their operations earn twice as much as those who use it less.[29]

Access to the Internet is a major contributor to economic growth. Slowing down access expansion has significant costs: research suggests that a 10% increase in Internet penetration is correlated with a 1% increase in the annual rate of new business formation. The Internet can be instrumental in SME growth in developing countries, as evidenced by the success of e-commerce companies like the online marketplaces Alibaba.com in China and Flipkart in India.[30]

26 McKinsey Global Institute, Global Flows in a Digital Age: How Trade, Finance, People and Data Connect the World Economy (2014)

27 SMEs on eBay are almost as likely to export as large businesses, have a 54% survival rate compared with offline businesses (24%), and over 80% of these businesses export to five or more countries. See: Andreas Lendle, Marcelo Olarreaga, Simon Schropp and Pierre-Louis Vézina, There Goes Gravity: How EBay Reduces Trade Costs International Trade and Regional Economics Discussion Paper No 9094 (August 2012) Centre for Economic Policy Research

28 Ibid

29 Deloitte Access Economics, Connected Small Businesses: How Australian Small Businesses are Growing in the Digital Economy (2013)

30 Economic Times, Flipkart raises US$200 million in single-largest round of funding in Indian e-commerce space. (July 11, 2013)

Cross border data flows also promote trade finance and SME access to capital. Modern, cross-border credit information systems encourage competitive access to credit for consumers and SMEs, level informational playing fields, and improve underwriting and market access. Unimpeded data flows are crucial to this process.[31] A survey of 4,800 SMEs in 12 countries finds that SMEs utilising the Internet for business functions grew at twice the rate of those that did not.[32]

The Internet also opens up new sources of credit and financing for SMEs. In Asia, for example, there are different experiments with developing non-bank-lending sources for SMEs. The China Hi-Tech Property Exchange, which provides stock equity transfer, venture capital investment, as well as an information platform for investors and SME issuers/borrowers is an experiment in equity investment for SMEs. Measures that diversify such dependence on banks, including crowd funding, peer-to-peer financing, and leasing, among other sources may ensure more sustainable sources of funding for SMEs.[33] These new models depend on easy access to information.

SMEs benefit from greater information transparency and information integrity. An example of this is the creation of credit databases.[34] Lenders have greater access to information about SMEs through the use of more standardized credit reporting across geographic borders. This can lower transaction costs for both the lenders and borrowers.

Internet and technology-based transactions have opened up global markets and customers and suppliers for SMEs through business-to-customer and business-to-business models such as e-Bay. Technology can improve access to information and reduce transaction costs. For example, Alibaba (the Chinese online marketplace) has harnessed the data generated from its Internet business in order to gain a solid understanding of the credit risk of its customers, having extended as of July 2013, over RMB100 billion (US$16 billion) to more than 320,000 small businesses in three years.[35]

Innovative technology-based SME business and financing require proper government policies to ensure a level playing field. The Korean government adopted nationwide broadband in 2000 as

---

Nathan Associates and FICCI, Unleashing the Potential Internet's Role in the Performance of India's Small and Medium Enterprise (2013)

31 Asean SME Working Group, BEYOND AEC 2015: Policy Recommendations for ASEAN SME Competitiveness (August 2014), p34

32 James Manyika and Charles Roxburgh, The Great Transformer: the Impact of the Internet on Economic Growth and Prosperity (McKinsey Global Institute, October 2011).; See also Manyika, James, Eric Hazan, Jacques Bughin, Michael Chui, and Rémi Said, Internet matters: The Net's sweeping impact on growth, jobs, and prosperity (McKinsey & Company 2011)

33 ASEAN SME Working Group, supra note 38 and Accountants for Business, SME Financing, supra note 40. The European Commission recognised the potential of crowd funding to complement traditional financing channels and indicated its intention to support it in its 2013 Green Paper on Long-term Financing for SMEs. A public consultation with stakeholders carried out later the same year fed into the communication on crowd funding published in March 2014. While the Commission does not currently envisage taking legislative measures, it aims to explore the added value of EU action. This includes raising awareness, creating a European 'quality label' for platforms and developing best practices, notably through setting up the European Crowdfunding Stakeholder Forum, as well as assessing the EU and national regulatory frameworks.

34 Association of Certified Chartered Accountants, Accountants for Business, Innovations in Access to Finance for SMEs (2014), p8; UNCTAD, The Role of Finance To Enhance Enterprise Development, Improving the Competitiveness of SMEs in Developing Countries (2001); UNCTAD has since published Entrepreneurship Policy Framework and Implementation Guidance (2012)

35 Ibid

a deliberate policy to establish Korea as a leader in e-commerce and become the world's most connected society.

The Internet is creating new opportunities for SMEs and for businesses in developing countries to engage in international trade and become part of the global economy. By providing opportunities to access business inputs such as cheaper telecommunications, strategic information on overseas markets, legal and consulting services, and cloud computing, SMEs and developing country firms are now more than ever able to become globally competitive.

In Focus: The Importance of ICTs for SME's in Kenya

The African telecom industry is growing rapidly. Investment is bypassing fixed-line (or "landline") services and focusing on mobile technology. One of Africa's innovation success stories has been the M-PESA system, which was introduced by Vodafone and launched by Safaricom in 2007, which enables mobile money transfer. It has had an extremely positive impact on the ability of Kenyans to transact, pay, and earn, and has transformed the ways of doing business as well as enhanced financial inclusion, particularly for the large numbers of Kenyans who do not have a bank account. By mid 2015, almost 29 million Kenyans used mobile money transfers provided by several mobile operators out of a population of 45 million.[36] Accordingly, local online trading solutions have been developing. For example, using Ebay is difficult in Kenya as most Kenyans don't have credit cards or bank accounts to link to PayPal, making it harder for them to conduct transactions. Kenyans instead mostly use a service called OLX (local online classified ads service), which allows M-PESA payments.

An important sector for the Kenyan economy is agriculture. There are several successful examples of companies applying ICTs to solve agricultural problems and boost trade. One such example is the application MFarm, which improves price transparency for crops and market access for farmers.[37] Most Kenyan farmers are small-scale producers accustomed to having only one source of information about the price of crops – their buyer. This often led to small farmers getting below-market value for their crops as they had little or no access to other buyers or to actual retail pricing.

MFarm filled that information gap by developing a simple system based on text messages (SMS), which sends pricing information to subscribers on 42 crops sold in 5 markets. The app also gives information on buyers and on "group selling", so that small-scale farmers can get together and command a better price. Transactions are powered by MPESA and MFarm takes a small transaction fee. A study in central Kenya with 600 farmers showed that farmers could double their sales by using MFarm.[38]

36 Communications Authority of Kenya, First Quarter Sector Statistics Report for the Financial Year 2015/2016 (July- September 2015)

37 http://www.mfarm.co.ke/

38 Olivia Solon, MFarm empowers Kenya's farmers with price transparency and market access, Wired (21st June 2013)

Implications for Global Trade Agreements

Trade agreements and policies have become an important source of rules governing cross-border information flows. One of the reasons free flow of data has become such an important part of international trade negotiations is the potential for economic benefits discussed in previous sections – in particular benefits for small businesses and traders.

The US and the Republic of Korea were the first states to include principles related to Internet openness and Internet stability in the electronic commerce chapter of the US/Korea FTA (referred to as KORUS FTA). Article 15.8 of the agreement says "the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[39] However, the KORUS FTA provision does not forbid the use of such barriers, nor does it define necessary or unnecessary barriers. Thus, a party could likely justify using such barriers under WTO exceptions to protect its consumers.

Today, the free flow of data is a key issue under debate in three ongoing trade treaty negotiations: The US and the 28 nations of the EU have been negotiating T-TIP (the Transatlantic Trade and Investment Partnership); the US and 10 other nations bordering the Pacific have signed the Trans-Pacific Partnership (TPP), now headed for ratification; and some fifty members of the WTO, including EU member states are negotiating the Trade in Services Agreement (TiSA).

In 2011, the US government proposed language in the TPP, which could enhance Internet openness.[40] It wanted to include language obligating TPP countries not to block the cross-border transfer of inbound and outbound data over the Internet.[41] Additionally, the US has pushed rules prohibiting countries from requiring data servers to be located in their country as a business condition, as well as provisions allowing businesses to operate in countries via e-commerce platforms, without establishing a commercial presence in the country.

During the negotiations, officials from some of the TPP parties did not respond positively to these provisions. Some countries in the negotiation, such as Vietnam, currently have extensive restrictions on the Internet. (See Box 5 below.) Moreover, some fear requirements that e-commerce platforms not be located at home is a national security issue. In the final agreement, the twelve TPP signatory countries committed in the Electronic Commerce chapter to ensuring free flow of the global information and data that drive the Internet and the digital economy, subject to exceptions for legitimate public policy objectives such as personal information protection.[42]

The US and the EU are also negotiating a new trade and investment agreement, referred to as the Transatlantic Trade and Investment Partnership or T-TIP. The aim is to develop new rules on "21st century" issues in the T-TIP. This may include addressing barriers to digital trade, such as the appropriate balance between the free flow of information and the right of governments to

39 Office of the United States Trade Representative, KORUS FTA (December 2010)

40 Office of the US Trade Representative, Trans-Pacific Partnership: Summary of US Objectives (2011)

41 Ian F. Fergusson, Mark A. McMinimy and Brock R. Williams, The Trans-Pacific Partnership (TPP) Negotiations and Issues for Congress, Congressional Research Service Report R42694 (March 20, 2015), pp. 40-41

42 Office of the US Trade Representative, Summary of the Trans-Pacific Partnership Agreement

regulate data flows, and between protecting personal data and permitting access to that data for law enforcement purposes.[43]

At the WTO, the Trade in Services Agreement [44] (TiSA) is being negotiated to update international standards since the General Agreement on Trade in Services (GATS) agreed more than 20 years ago. The negotiations are taking place as increased use of the Internet has dramatically changed the global services market. Negotiators must therefore consider the changes created by the digital revolution. GATS does not explicitly address the growing practice of requiring local storage and processing of business data. The US has tabled provisions focused on the free flow of data in TiSA, as well as prohibitions on data localisation requirements.45 The EU has stated that any free flow provisions will not undermine EU privacy laws, namely the EU Data Protection Directive[46] (see Section 2.6 below).

Implications for Human Rights

Restrictions on the free flow of information not only hinder economic growth; they can also lead to adverse human rights impacts. These include adverse impacts on freedom of expression and the rights to privacy, which are both enshrined in the International Covenant on Civil and Political Rights (ICCPR).

There are other harms that come from limiting data flows. To the extent that only some types of companies or businesses have access to the Internet or technology (e.g. those who can afford a service, or are willing to register), it discriminates in favour of particular classes of entrepreneurs, and result in adverse effects on other entrepreneurs with poorer access to resources, which could include small businesses run by women, minorities, and marginalised or economically vulnerable groups. Filtering or censorship may have a similar impact in terms of who is willing to use technology. Article 26 of the ICCPR affirms the right to be free from discrimination and Article 22 protects the right of individuals to associate freely. This right protects those wishing to join like-minded individuals in Internet-based groups, as a means of collectively expressing beliefs. To the extent that ICT and data flows are restricted, this adversely impacts freedom of association, whether it is workers who wish to organize, or groups of entrepreneurs banding together as a trade association.

The International Covenant on Economic, Social and Cultural Rights (ICESCR) recognises an individual's right to work (Article 6) and the right to an adequate standard of living (Article 11). If a person's livelihood is adversely impacted by the curtailment of access to information, this would be a denial of essential economic rights enshrined in the ICECSR. The ICECSR also provides the right to form unions (Article 8) and asserts consistency between the ICESCR and state duties as parties to the ILO Convention concerning freedom of association and protection of the right to organise. To the extent that workers are unable to communicate via the Internet, this also impacts their rights of association. In particular, the ICESCR addresses the issue of economic burdens imposed by a restricted and localised Internet.

43 Shayerah Ilias Akhtar and Vivian C. Jones, Proposed Transatlantic Trade and Investment Partnership (T-TIP): In Brief (Congressional Research Services June 2014)

44 Peter Allgeier, President, Coalition of Service Industries, What is TiSA and Why Does it Matter? (International Trade Forum, April 15, 2014)

45 Inside US Trade, US Tables New TiSA Proposal To Ensure Free Flow of Data, (15 May 2014);

TechDirt, New TISA Leak: US On Collision Course With EU Over Global Data Flows (December 17, 2014).

46 Aronson, Why Trade Agreements are not Setting Information Free, supra note 4, at pp.2-3

The ICECSR also recognizes the right to take part in cultural life and to enjoy the benefits of scientific progress and its applications. If a particular technology or use of the Internet is banned or limited, rights relating to access to information are infringed, also preventing the use of that technology as a source of innovation.[47]

Costa Rica, Estonia, Finland, France, Greece, and Spain have asserted some right of access in their constitutions or statutes, or via judicial decisions.[48] UN Special Rapporteurs on freedom of expression from the United Nations (UN), the Organisation of Security and Co-operation in Europe (OSCE), the Organisation of American States (OAS) and the African Commission on Human and People's Rights, have all concluded that cutting off access to the Internet can never be justified under human rights law, including on national security grounds.[49] The OECD has noted that the Internet:

> *"allows people to give voice to their democratic aspirations, and any policy making associated with it must promote openness and be grounded in a respect for human rights and the rule of law."*[50]

The Council of Europe has also affirmed a commitment to access as a right.[51] A recent survey of 13 countries found that a majority of respondents (over 70%), especially participants from developing countries, viewed Internet access as a fundamental right.[52]

47 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, May 16, 2011, UN Doc. A/HRC/17/27

48 David Rothkopf, Is Unrestricted Internet Access a Modern Human Right? Foreign Affairs, February 2, 2015. La Rue, supra note 61

49 UN, OSCE, OAS, African Commission on Human and People's Rights, Joint Declaration on Freedom of Expression and the Internet (2011) Article 6b

50 OECD, OECD Council Recommendation on Principles for Internet Policy Making (December 13, 2011)

51 Council of Europe Convention no. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Preamble and Article 12). Strasbourg, 28.I.1981; see also Anupam Chander, International Trade and Internet Freedom 102 Am Society Int'l Proc. 37 (2009)

52 Soumitra Dutta, William Dutton and Ginete Law, The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online, Global Information Technology Report (2010-11), p9

II. Threats and Obstacles to Cross Border Trade and the Free Flow of Information

The IHRB discussion paper "No Trade Off" presented at the Stockholm Internet Forum in 2014[53] identified and analysed emerging trends concerning restrictions on the free flow of data. This section provides an update on these issues and takes a more in-depth look at examples from around the world to illustrate threats, obstacles, and opportunities. The specific trends and examples discussed are:

- Data localisation/storage requirements
- Encryption
- Content censorship through blocking/filtering
- Requirement for Internet users to register with the government
- Connectivity and access
- Data protection through restrictions on cross border data flows to protect data and privacy

Data Localisation/Storage Requirements

One key phenomenon that has changed the trading landscape for business and consumers alike is the development of "cloud computing".[54] The cloud makes storage of large amounts of data on a personal computer system no longer necessary. Businesses won't have to invest in their own technology infrastructure; instead they can access data and Internet services via a third party. Data can now be stored on remotely located servers, and accessed over the Internet. This permits users almost unlimited amounts of data storage, accessible from any computer. Cloud storage is most commonly used for email (such as Gmail) and storing data (such as Dropbox).

The location of stored data has become a key point of debate, and the issue of data localisation has emerged as an issue of major concern for business and civil society. There are two aspects to data localisation: On one hand, users and businesses may be able to *choose* where their data is stored, lowering costs for businesses and giving users more control over their data. On the other hand, some States are forcing companies to store data on servers within their jurisdiction, as will be discussed below. Forced localisation increases costs for international companies as they must locate or develop the facilities to store data, and adversely impacts local businesses if they cannot access services outside their own borders. Forced localisation also raises serious human rights concerns with respect to who can access data and under what circumstances. Here we analyse both sides of the debate.

53 IHRB (2014) Discussion Paper: No Trade Off. Restrictions on the Free Flow of Data, World Trade and Human Rights

54 In the simplest terms, cloud computing means accessing files and applications over the internet, rather than on personal hard drives or servers, via third party services.

Within weeks of the publication of documents leaked by Edward Snowden in June 2013, revealing mass surveillance practices of several governments, it was reported that US technology companies were losing business to overseas competitors. The majority of the companies associated with the leaked documents are based in the United States. Much discussion focused on the access of user data by the US NSA with or without the knowledge of the companies in question. Users of data storage services, such as cloud computing and web-hosting inside the United States seemed to have acted quickly to switch to non-US providers in countries perceived to be more 'neutral' or with stronger data and privacy protections. A report by The New America Foundation on the financial costs of NSA surveillance stated that "[T]he CEO of ArtMotion, one of Switzerland's largest offshore hosting providers, reported in July 2013 that his company had seen a 45% jump in revenue since the first [mass surveillance] leaks."[55]

An August 2013 study by the Information Technology and Innovation Foundation (ITIF) estimated that revelations about the NSA's PRISM program, where the NSA obtained direct access to several technology companies' servers, could cost the American cloud computing industry $22 to $35 billion over the next three years. On the low end, the ITIF projection suggests that US cloud computing providers would lose 10% of the foreign market share to European or Asian competitors, totaling in about $21.5 billion in losses; on the high-end, the $35 billion figure represents about 20% of the companies' foreign market share.[56]

Elsewhere, companies began marketing services based on their home country's perceived strong privacy protections (such as F-Secure in Finland[57]) or capitalising on the fact that data was not stored in the US (such as Deutsche Telekom's *Email Made In Germany* service[58]). Amazon, Salesforce, IBM and Oracle are proactively setting up data centres in Germany. Companies like Amazon reportedly admit that they are driven to relocate data centres, in part, by political pressure to regain trust with European customers.[59]

A memo from the European Commission outlined the importance of cloud computing, and how the surveillance revelations had presented challenges, but that it should be turned into a "*Europe-wide opportunity: for companies operating in Europe to offer the trusted cloud services that more and more users are demanding globally*".[60]

However, at the end of 2014, according to the European Union statistics office Eurostat[61], only one in five businesses in Europe used cloud computing for email and storage. A main factor for businesses not using cloud computing was down to lack of knowledge (42%), closely followed by concerns over security (37%). A third factor was concerns about the uncertainty over the location of data and applicable laws. In developing countries, cloud usage is lower still. Some of

55 New America Foundation Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom and Cybersecurity, (July 2014) p.7-8 citing the source David Gilbert, Companies Turn to Switzerland for Cloud Storage Following NSA Spying Revelations, International Business Times, (July 4th 2013)

56 Daniel Castro, How Much Will PRISM Cost the US Cloud Computing Industry? The Information Technology and Innovation Foundation (August 5th, 2013); New America Foundation, Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom and Cybersecurity (July 2014); Murad Ahmed, Amazon to open German data centres to soothe European concerns, Financial Times (October 23rd 2014)

57 http://safeandsavvy.f-secure.com/2013/10/07/would-you-trust-finland/#.UuE_R6U4k_M

58 http://www.e-mail-made-in-germany.de. See also Mark Scott, European Firms Turn Privacy Into Sales Pitch, The New York Times, (June 11 2014)

59 Katharine Kendrick, Risky Business: Data Localisation, Forbes, (February 15, 2015)

60 European Commission memo, What does the Commission mean by secure Cloud computing services in Europe? (15 October 2013)

61 EuroStat News Release, Cloud computing services used by one out of every five enterprises in the EU28 (9 December 2014)

this due to lack of proper broadband infrastructure to facilitate cloud computing. Another reason cited by the UN Commission for Trade and Development relates to the lack of clear and strong regulatory frameworks relating to cloud computing.[62]

These user concerns are fueled by both mass surveillance revelations, and the high profile security breaches of companies like Sony[63], Apple's iCloud[64] and the UK ISP Talk Talk[65] where users' personal details such as passwords, credit card numbers, and photos were leaked online.

There is no guarantee that data under "local" supervision is safer than in a cloud stored elsewhere. Lost trust in one country does not mean that another location is more trustworthy merely because it makes such a claim. That model rests on the assumption that other governments would not themselves misuse their control over such data, or that data is "out of reach". In addition, storing data locally does not solve the need for strengthened privacy or data security. In April 2015, several prominent technology companies, including web hosting and technology companies OVH, IDS, and Gandi threatened to pull out of France in the wake of the introduction of a bill they argue will put the entire French population "under surveillance." They addressed a letter to the French Prime Minister, stating that they will be sent into de facto "exile" if the French government legislates the "real-time capture of data" by its intelligence agencies in the wake of the attacks on the offices of the French satirical magazine Charlie Hebdo in January 2015.[66]

This loss of trust in cloud services following state surveillance revelations is compounded by legislation that fails to take into account the global nature of cloud computing, leading to confusion about who can access data and for what purpose. This is particularly relevant for criminal investigations. Only a few years ago, US based e-mail providers held their data in the United States, so there was no issue of whether a court had jurisdiction to issue a warrant for the data. As more US companies host massive amounts of data from customers around the world, they have begun to store much of that information overseas. This ensures that clients abroad get access to their data, videos and e-mails without delay. For European clients, data storage in Europe gives them confidence that their records will be subject to European laws. The proposal to allow customers to *choose* where they store their data seemed to be a positive step forward in restoring trust and giving users some control and ownership of their personal data. In late 2013, Microsoft began giving customers (initially business customers) the option of storing their data in Microsoft's data centres around the world. Microsoft has about 100 such facilities in 40 countries. Privacy advocates welcomed the move.

62 UNCTAD, Information Economy Report 2013: The Cloud Economy and Developing Countries

63 Sony Playstation was hacked several times in 2011, but it was the theft of details from 77 million user accounts which led to Sony being fined £250,000 by the UK's data protection watchdog for not doing enough to protect user data. Ben Qu8inn and Charles Arthur, PlayStation Network hackers access data of 77 million users, The Guardian (26 April 2011); Out-Law.com, ICO fines Sony £250,000 over security failings that exposed 'millions' of UK customers' personal data, (24 Jan 2013). In 2014, Sony Pictures systems were hacked, reportedly by North Korea, resulting in the leaking of employee details, emails, yet-to-be-released films. The incident also led to a lively debate on major media companies and freedom of expression, with Sony first withdrawing, and then screening, a film to which North Korea had objected, and whose potential release was believed to be a probable cause for the hack. Vlad Savov, Sony Pictures hacked: The Full Story, The Verge (December 8 2014)

64 Charles Arthur, Naked celebrity hack: security experts focus on iCloud backup theory, The Guardian (September 1 2014)

65 BBC News Online, Customer data stolen in Talk Talk hack attack (February 27 2015)

66 OVH, IDS and Gandi, Le gouvernement veut-il contraindre les hébergeurs Internet à l'exil? OVH News, (April 9 2015)

Around the same time, a US federal judge served a warrant on Microsoft to obtain information relating to an email account stored on the company's servers in Ireland regarding an investigation into drug trafficking. Microsoft refused to comply, arguing that a US warrant was not valid in other countries and the request should at the very least go through an MLAT process (See Annex 1 on MLATs). Microsoft stated in a brief to a US Court:

> *"Congress has not authorised the issuance of warrants that reach outside U.S. territory… The government cannot seek and a court cannot issue a warrant allowing federal agents to break down the doors of Microsoft's Dublin facility."*[67]

Microsoft refused to turn the emails over to the government and challenged the warrant, arguing that a federal magistrate judge had no authority to issue a search warrant for records stored abroad. Microsoft lost this first appeal in April 2014. Microsoft appealed for a second time to the US District court and argued that the US government needed to request the information via the US-Ireland Mutual Legal Assistance Treaty (MLAT) process. The District court rejected Microsoft's appeal in July 2014. Microsoft lodged a third appeal in December 2014 to the US Court of Appeals for the Second Circuit, which was heard on 9 September 2015, with support from the government of Ireland and numerous technology and media companies, trade associations and advocacy groups.[68] During the appeal the United States Department of Justice argued that it has the right to demand the emails of anyone in the world[69] from any email provider headquartered within US borders.

Microsoft backed US legislation proposed in September 2014[70], the Law Enforcement Access to Data Stored Abroad Act (LEADS), which would set limits on the kind of information the government can force US companies to hand over when it is stored overseas. The government would only be able to obtain a warrant relating to US citizen's data stored overseas and not foreigners.[71] The Bill was introduced in February 2015 and at the time of writing has yet to be introduced to the Senate.[72]

As discussed in Annex 2, in 2015 the Court of Justice of the European Union (CJEU) ruled in *Schrems versus Data Protection Commissioner*, that the EU-US "Safe Harbour" agreement, which allows for cross border data transfers between the EU and the US, is invalid and in violation of European data protection regulations. In October 2015, Microsoft made a supplemental filing with the appeals court in the United States, arguing that the case is relevant, Microsoft urged the court to take into account the CJEU's invalidation of the Safe Harbour data transfer scheme as well as a recent US Senate hearing[73] on electronic privacy laws, when ruling on whether to allow the US law enforcement to access consumer data stored overseas.[74] The US Department of Justice responded with a letter claiming that the CJEU decision focuses solely on voluntary data transfers and is irrelevant to the Irish case, which is

67 Electronic Frontier Foundation (EFF), In re Warrant for Microsoft Email Stored in Dublin, Ireland

68 Rebekah Mintzer, Corporate Counsel, Stormy Weather? Microsoft Ireland Case Stirs Fears About the Future of Cloud (September 1 2015)

69 Sam Thielman, Decision in Microsoft Case Could Set Dangerous Global Precedent, Experts Say, The Guardian (9 September 2015)

70 Microsoft Corporate Blog, New milestone in the conversation about electronic privacy laws (September 18 2014)

71 Mario Trujillo, Justice Department gets earful from Congress over Microsoft case, The Hill (February25 2016)

72 Track the progress of the bill here

73 Allison Gande, Microsoft Flags EU Data Pact Demise in Fight over Warrant, Law 360 (October 7, 2015)

74 Ibid

focused on law enforcement's request for information, and that the company's reliance on the Safe Harbour decision in the *Schrems* case was misguided.[75]

At the time of writing, the court had yet to reach a decision and the case continues. This is a real-time legal battle that tech companies are watching closely.[76] It raises both legal compliance questions and business concerns. Under what authority may the US government seize the personal data of a company's customers in other countries? If Microsoft loses, will other countries attempt to seize data held on US servers? If users fear that their data will be subject to search and retrieval by the countries in which they are headquartered, as is the case with Microsoft, they may move their data based on which jurisdictions provide greater protections. Thus, there is need for governments to clarify what should be the correct procedures to access data stored outside of their territory. Brad Smith, Microsoft's general counsel and executive vice president of Legal and Corporate Affairs said,

> *"Law enforcement needs to be able to do its job, but it needs to do it in a way that respects fundamental rights, including the personal privacy of people around the world and the sovereignty of other nations."*[77]

Annex 1 describes a possible way forward with mutual legal assistance treaties, or MLATs, where information relating to criminal investigations can be shared between countries or regions parties to the agreement. These agreements could be reformed to provide a solution for cross-border data sharing, but currently the MLA process applies only to criminal investigation, and not to intelligence gathering. Any suggestion of expanding the MLA process to intelligence agencies, given the current sensitivities around surveillance, would require particular scrutiny and consultation.

It is clear that the issue of cross-border access and storage of data and jurisdiction is central in the ICT, trade, and human rights debate. The battle for data control will continue, as innovation and trade exigencies will militate against existing legal frameworks, which remain inadequate in dealing with the pace of change in the digital age.

Forced Data Localisation and its Economic and Human Rights Impacts

The cases described so far rested on the assumption that users may be able to choose where to store their data. But there is another challenge, as some states are starting to *force* companies to store data pertaining to their citizens within their borders. Before the 2013 mass surveillance disclosures, the issue of states forcing companies to store data locally existed but was not central to the global debate. But it is now clear that forced localisation means forced jurisdiction. Legal requirements on companies to store data on servers placed inside a particular country raise concerns for both trade and human rights.[78]

75 Allison Grande, EU Data Ruling Moot In Microsoft Warrant Fight, DOJ Says, Law 360 (October 19, 2015)

76 See updates on the case here: http://digitalconstitution.com/

77 Brad Smith, Our legal challenge to a U.S. government search warrant, Digital Constitution (9 April 2015)

78 Stephen Ezell, Robert Atkinson and Michelle Wein, Localisation Barriers to Trade: Threat to the Global Innovation Economy, Information Technology and Innovation Foundation (ITIF) (September 25 2013)

Proponents of data localisation argue that doing so would keep data "safe", demand improvement of a country's ICT infrastructure, and that, in turn, would boost the economy.[79] In contrast, the Swedish Ministry of Trade's paper "No Transfer, No Trade" identified regulation over data localisation as the main concern of the Swedish companies interviewed, in particular restricting data from being moved out of the country:

> *"A central problem for companies is how data regulation, especially restrictions on moving data to third countries, could entail missed business opportunities by increasing costs and inducing delays, making companies' prices unattractive or making products late to market."*[80]

In 2012, the Business Roundtable reported that 13 countries had data localisation laws[81] either passed or under proposal, which, according to an Open Technology Institute report, "would prevent or limit information flows."[82] The report also explored how forced data localisation would be seen as an attempt by governments to exert more control over citizens with potentially adverse human rights impacts. This could mean making databases of human rights organisations, political dissidents, or other activists susceptible to surveillance from home governments that have a poor human rights record. Corporate decisions regarding locating employee data could also be affected if it involves countries where employees may face discrimination due to their sexual orientation, religious or ethnic background, or political beliefs, if such records are kept and accessible. Information all gathered in one place may make it easier to access data – not just for surveillance but also for cyber-criminals committing fraud and identity theft.

In Focus:
Brazil: Reacting to Surveillance Allegations and the Potential Economic Impact

A recent study by the European Centre for International Political Economy (ECIPE) developed economic models to assess the impact of forced data localisation laws in various economies. The study concluded that the impact on GDP from recently proposed

79 Anupam Chander and Uyen P. Le, Breaking the Web: Data Localisation vs. the Global Internet, UC Davis School of Law Research Paper No. 378, April 2014

80 Kommerskollegium, The National Board of Trade, No Transfer, No Trade- The

Importance of Cross-Border Data Transfers for Companies Based in Sweden (January 2014), p2

81 The countries are Australia, Brunei, China, Greece, India, Indonesia, Malaysia, Nigeria, Russia, South Korea, Ukraine, Venezuela and Vietnam. See: Business Roundtable, Promoting Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements (June 2012), p5-6. (At the time the report was published, the Business Roundtable noted that while the stated rationale was national security, there are "indicators of industrial policy motivation" among the states imposing localisation requirements)

82 Anupam Chander and Uyen P. Le, Breaking the Web: Data Localisation vs. the Global Internet, UC Davis School of Law Research Paper No. 378, April 2014

or enacted legislation in this area is substantial in the seven countries/regions studied: Brazil, China, EU, India, Indonesia, Korea and Vietnam. Brazil has been one of the most vocal critics of mass surveillance revelations and its response among the most robust.[83] Brazil's president urged the Brazilian Congress to give attention to a bill of Internet rights, the *Marco Civil,* which was first proposed in 2009.[84] In earlier drafts, it included a proposal to add local data storage rules for foreign companies, but this was dropped from the final text. However, according to ECIPE, an element of data localisation remains that could be damaging to Brazil's economy. According to ECIPE:

> *"The bill still contains a provision that stipulates that online service providers need to comply with Brazilian law when active in Brazil, even if they are based abroad. This would allow the Brazilian government to access data on their own citizens held by foreign companies through a simple court order."* [85]

A further ECIPE research paper [86] concluded that introducing economy-wide data localisation requirements that apply across all sectors would result in even larger GDP losses. It said that these measures would,

> *"…decrease the country's GDP by -0.2% in 2014. If Marco Civil had introduced a cross-sector data localisation measure, as originally intended, the negative effects on GDP would have quadrupled (0.8%). It would have also had a severe impact on investment (-4.2%), as the country's competitiveness would decrease, leading jobs to shift to other economies in the region."*

Further, the impact on overall domestic investments is also considerable. The report also found that welfare losses (expressed as actual economic losses by the citizens) amount to up to $63 billion for China and $193 billion for the EU. For India, the loss per worker is equivalent to 11% of the average month salary, and almost 13% in China and around 20% in Korea and Brazil.87

According to the New America Foundation[88], other new measures proposed by the government of Brazil to protect citizens from NSA surveillance are:

- Increasing domestic and international Internet connectivity.
- Encouraging domestic content production and the use of network equipment built in Brazil.
- Abandoning Microsoft Outlook in favour of a domestic email system that relies on data centres located only in Brazil.

83 Jonathan Watts, NSA accused of spying on Brazilian oil company Petrobras, The Guardian, (September 9 2013)

84 Marco Civil da Internet (English)

85 Bert Verschelde, The Economic Impact of Marco Civil da Internet in Brazil, ECIPE Bulletin No. 06/2014

86 Matthias Bauer, Hosuk Lee-Makiyama Erik van der Marel & Bert Verschelde. The Costs of Data Localisation: Friendly Fire on Economic Recover, European Centre for Informational Political Economy Occasional Paper No. 3/2014 (2014).

87 Ibid. See also Hill, supra note 58

88 New America Foundation, Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom and Cybersecurity (July 2014) pp 16-17

- Building a new undersea cable between Brazil and Europe, circumventing the US and avoiding using US contractors to build it. The estimated cost is $185 million.[89]

Impact of Data Localisation on Business

If ICT companies were forced to locate servers locally in different jurisdictions, this would add layers of complexity for business, as companies may have to build data centres in more countries (under different jurisdictions). This could build redundancies and add to business costs, making it harder for companies to serve customers in some parts of the world and making costs prohibitive for SMEs and start-ups, which will be restricted in the choice of services due to less competition and reduced access to global services.[90] It will also impact consumers whose costs would probably rise.

A larger question concerns whether building data centres in different locations is necessarily a prudent or efficient means of investment. Data centres are expensive to build and operate. Countries pushing for data localisation may not have the systems to securely store data, or the necessary expertise within the country to ensure security, which would make data vulnerable and at risk of being hacked.[91] Maintaining such high-tech hardware in developing countries that lack adequate power to provide other essential services to their populations such as hospitals is also a matter of serious concern.

Impact of Data Localisation on Internet Structure

According to experts, forced data localisation creates complications for the international architecture of the Internet. Data packets flow without recognising political boundaries and borders. Restricting how these packets can move poses significant logistical problems. As the New America Foundation report outlines:

> *"Data localisation proposals also threaten to undermine the functioning of the Internet, which was built on protocols that send packets over the fastest and most efficient route possible, regardless of physical location. If actually implemented, policies like those suggested by India and Brazil [detailed later in the study] would subvert those protocols by altering the way Internet traffic is routed in order to exert more national control over data."*[92]

Ultimately, security researchers believe this focus on the physical location of data as a security mechanism is counter-productive and that in fact, data privacy and security depends primarily

89 Nancy Scola, Brazil begins laying its own Internet cables to avoid US surveillance, The Washington Post (November 3 2014)

90 Anupam Chander and Uyen P. Le, Breaking the Web: Data Localisation vs. the Global Internet, UC Davis School of Law Research Paper No. 378 (April 2014)

91 Rajkumar Buyya1,2, Anton Beloglazov1, and Jemal Abawajy, Energy-Efficient Management of Data Center Resources for Cloud Computing: A Vision, Architectural Elements, and Open Challenges (2012)

92 New America Foundation, Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom and Cybersecurity (July 2014) p19

on how it is stored and transmitted, and not where it is located. As security researchers have pointed out,

> *"Betting on these ill-conceived initiatives [of data localisation] risks wasting important resources that could be used for more promising proposals to effectively make data more secure, namely greater use of and better encryption."*[93]

Encryption is another politically charged issue and the focus of the next section.

In Focus: Data Localisation in Russia

As part of a wider set of laws aimed at tightening government control over the Internet, Russia amended existing data legislation in 2014 to require companies to store personal data of Russian citizens, including data collected on the Internet, on servers based inside Russia.[94]

Authorities described these measures as an attempt to prevent foreign spying on Russian citizens (President Vladimir Putin has described the Internet as a "CIA project"[95]). However, human rights advocates are concerned that these powers give the Russian government more control over Russian citizens' personal data and the government will have more opportunities to impose surveillance, which would have been more difficult if the data was stored in other jurisdictions.

It has been reported that Russia has been updating its SORM[96] system of surveillance to allow collection and storage of all mobile and online communications[97], and that a high degree of surveillance was in place at the 2014 Winter Olympics in Sochi.[98] Amid tightened restrictions, Google closed down its office in Moscow at the end of 2014.[99]

93 Tim Maurer, Robert Morgus, Isabel Skierka, The anti-surveillance strategies that could ruin the Internet, TIME, (December 10 2014)

94 LinkLater, Russia: New Data Localisation Law: Current State of Play (December 8 2014)

95 Ewen MacAskill, Putin calls Internet a "CIA project" renewing fears of web breakup, The Guardian (April 24 2014)

96 SORM (literal translation, System for Operative Investigative Activities) is a surveillance system that allows security services tap into and monitor all mobile phone communications in real time. The modernising of the SORM system can be charted from the Soviet-era system that prevailed in the 1980s, when SORM was established to intercept fixed line communications. In 1996, SORM 1 was established to intercept fixed line and mobile communications. Two years later, SORM 2 was established to allow additional monitoring of the Internet, including emails and VOIP. Some reports (see below) say that Internet Service Providers (ISPs) and operators were required to install a "black box" on the network, which would allow the secret service to intercept communications directly. Around 2012 SORM 3 was established to allow collection and long-term storage of all other user communication data, including actual recordings and location.

97 James Andrew Lewis, Reference note on Russian communication surveillance, Centre for Strategic and International Studies (CSIS) (April 18 2014)

98 Roland Oliphant, Russia planning 'near total' surveillance of visitors, athletes at Sochi Winter Olympics, The Telegraph (October 6 2013)

99 Alec Luhn, Google to close office in Russia as Internet restrictions bite, The Guardian (December 12 2014)

The law came into effect on September 1st 2015 and will certainly boost Russia's digital economy, as it would compel foreign companies to rent storage space from Russian companies.[100] According to Russian law firm ALRUD, while the law is silent on the extra-territorial application for non-Russian companies, *"non-binding guidance has been published which suggests that the new law would apply to non-Russian companies that either operate in Russia through a legal presence or that 'target' Russian consumers through websites"*.[101] There does not appear to be restrictions on transferring and processing personal data from Russia to foreign jurisdictions, but at the point of collection, *"the personal data of Russian nationals should initially be placed in a so-called primary database, which must be located and used to process such data in Russia."*[102]

Encryption

Following the 2013 mass surveillance revelations, efforts by companies to increase encryption of online services have become the new scourge of governments, creating tensions between tech companies and law enforcement agencies. Leaked documents alleged that intelligence agencies may have been creating "back doors" into company servers, by tapping the connections between servers. For example, the NSA had reportedly intercepted data travelling between Yahoo! and Google's servers.[103] Companies were reportedly unaware that their data was being accessed in this manner. This may have offered intelligence agencies a temporary advantage but it destroyed trust between government authorities and companies, and has increased actions by companies to develop encrypted mechanisms to prevent such intrusions. By exploiting or creating vulnerabilities in the networks in order to extract user information, government agencies weakened security in systems as a whole[104] and strengthened the resolve of companies to combat it.

In response to this intrusion, companies began to make changes to their systems to boost security and encryption, which is the technique by which data (when in transit or when at rest on devices) is scrambled to make it unreadable without using specific passwords or keys. Encryption makes the task of interception much harder and company efforts in this area has been heavily criticised by government authorities. For example, the director of the US Federal Bureau of Investigation (FBI) attacked Apple[105] for introducing default encryption on its operating system for the iPhone. The new director of the UK GCHQ attacked tech companies as well, calling them "command-and-control networks of choice for terrorists and criminals."[106]

100 Paul Sonne and Olga Razumovskaya, Russia steps up new law to control foreign internet companies, Wall Street Journal (September 24 2014)

101 Slaughter and May Briefing October 2015, Russia's New Data Localisation Law

102 Ibid

103 Barton Gellman and Ashkan Soltani, NSA infiltrates links to Yahoo, Google data centres worldwide, Snowden document says, The Washington Post (October 30 2013)

104 Charles Arthur, Academics criticize NSA and GCHQ for weakening online encryption, The Guardian (September 16 2013)

105 Trevor Timm, Your iPhone is now encrypted. The FBI says it'll help kidnappers. Who do you believe? The Guardian (September 30 2014)

106 Robert Hannigan, The web is a terrorist's command-and-control network of choice, The Financial Times (November 3 2014)

UK Prime Minister David Cameron, following the attack on the office of the French satirical magazine *Charlie Hebdo* in Paris in which 17 people died, took the opportunity to reignite the debate on encryption. Cameron's comments were interpreted as a pledge to bring in new powers to either weaken online encryption so that intelligence agencies can intercept and read encrypted emails and messages, or ban encrypted messaging apps altogether.[107]

With encryption comes security of user data, authentication, confidentiality and consumer trust in services. People undertake an increasing amount of legitimate activities over the Internet that involve personal information, such as banking, buying and selling goods, filing tax returns, and so on. Encryption is important to keep personal data safe *from* criminals. Without encrypted transactions, e-commerce would not have grown rapidly.

Encryption is not just important for ensuring safe online transactions. The UN Special Rapporteur on the Right to Freedom of Expression concluded that encryption provides the privacy and security necessary to exercise freedom of expression in a digital age, which in turn may be essential for exercising other rights, such as economic rights, due process, freedom of association and assembly, and the right to life and bodily integrity.[108] Encryption technology also allows human rights defenders and other people at risk to communicate without the fear of their confidential communications being intercepted arbitrarily by intelligence agencies. Governments are already targeting some civil society groups because they use encryption and Internet security techniques.

One of the charges against the jailed Zone 9 bloggers in Ethiopia is their use of encrypted communication and participation in trainings on Internet security.[109] Such training is provided by the Berlin-based organisation Tactical Technology Collective, which has developed the popular tool, *Security In A Box*, a publicly available resource used by thousands of human rights defenders worldwide.

In 2015, a group of seven human rights activists in Morocco were arrested for "threatening the internal security of the State" for organising a workshop on citizen journalism. According to the Human Rights Foundation, the workshop which included training people to use the smartphone app StoryMaker, which allows users to assemble and publish stories as well as share them securely via mobile phones.[110] The charge carries a maximum sentence of five years in prison and large fines. At the time of writing, the activists' trial is on-going and has been postponed several times in 2016.

States wishing to build a digital economy should recognise that encryption is essential. Encryption can be technologically complex, with different features and characteristics. Governments should engage experts in business and civil society in the conversation and seek expert advice, instead of using blunt instruments such as banning or criminalising this important online tool.

107 James Ball, Cameron wants to ban encryption- he can say goodbye to digital Britain, The Guardian (January 13 2015)

108 UN OHCHR, Report of the Special Rapporteur on the Promotion and Protection of Freedom of Expression, David Kaye A/HRC/29/32, (May 22 2015)

109 See Charge 1, Specification 1 and 2. Translation available here.

110 Human Rights Foundation, HRF to Morocco: Drop Charges Against Human Rights Activists (February 4 2016)

Content Censorship through Filtering/Blocking

Online censorship has a direct impact on freedom of expression and access to information. Information control is commonly focused on content critical of the state, discussions on democracy, exposing corruption or providing independent news. Sometimes entire websites are blocked because the company running the site has refused to take down certain content.

There are too many examples of state-ordered censorship to note here but recent examples include the blocking of Twitter and YouTube in Turkey when audio recordings alleging corruption involving the Prime Minister circulated on the site.[111] In Pakistan, a band released a satirical song criticising military generals. The video was uploaded on video sharing site Vimeo, which in turn led to the site being blocked.[112] In Ethiopia, the only Internet service provider (ISP), the state-owned Ethio Telecom, has been filtering its Internet access for some time to suppress opposition blogs and other news outlets.[113]

While adverse impacts on human rights are often discussed in depth, the economic impacts of censorship or censorship acting as a trade barrier receive less attention. A study by ECIPE[114] from 2009 states:

> *"An online business has few operational assets but still accrues costs; if a web site is taken out of service for seven days, it will have an impact on revenue equivalent to 2% of total annual turnover."*

In addition, online platforms such as user-generated video or photo sharing websites can often be directly or indirectly linked to people's livelihoods. Artists, musicians, photographers and authors who publicise their work often use content sharing platforms, such as Flickr, Vimeo, YouTube, Twitter, and Wordpress. They can miss out on employment opportunities as a result of censorship, or lose out on revenue sharing models, if sites are blocked. Independent news agencies subject to censorship can suffer and lose advertisers when blocked.

Many legitimate restrictions on the flow of information on the Internet (such as child abuse images) are implemented at the level of Internet intermediaries, such as ISPs. Such restrictions may require ISPs or other intermediaries to take affirmative steps to block or filter information flows. Some countries require ISPs to block material, remove content in response to takedown notices, or remove search results. In some circumstances governments also impose civil or criminal liabilities on intermediaries, including content hosts and ISPs. Otherwise known as "intermediary liability", the trend of some governments to force online companies to 'police' the Internet continues. ISPs or content providers are often held legally responsible if they do not remove 'objectionable' or 'offensive' content on their platform (usually uploaded by others) rather than operating on a "notice and takedown" process.

111 Kevin Rawlinson, Turkey blocks use of Twitter after prime minister attacks social media site, The Guardian (March 21 2014)

112 Nighat Dad, 2013: A deadly year for Pakistan's Internet freedom, Index on Censorship (January 9 2014)

113 For more information see, Human Rights Watch, They Know Everything We Do: Telecoms and Internet Surveillance in Ethiopia (2014)

114 ECIPE Working Paper, Protectionism Online: Internet Censorship and International Trade Law (2009)

This burden might be bearable for Internet giants such as Google, but for smaller businesses this is crippling. A Dalberg report[115] noted the examples of an Internet entrepreneur in Turkey who estimated that the cost of complying with an increasingly restrictive set of rules regarding website content accounts for 15% of his total operating costs. His company has fought 250 lawsuits in the 14 years since it was founded. In February 2014, the Turkish Parliament approved a new Internet law which allows the government to block websites without a court order and obliges companies to store data on user activities for two years. The CEO of Ekşi Sözlük, one of Turkey's most popular social networking website, reportedly spends 1 day per month in court defending against vaguely worded takedown requests, resulting in substantial legal and management costs; moreover, failure to comply with the new Internet law provisions could result in a year in prison.[116] In Thailand, the 2007 Act on Computer Crime, which included broad provisions concerning intermediary liability, has led many service providers to conclude that the burdens of doing business outweigh the benefits. The owner of the user-moderated discussion forum 212cafe.com, for example, has opted to shut down the business.

Few experts have examined Internet censorship as a trade barrier. Blocking services such as Voice over Internet Protocol (VoIP), can be for commercial reasons in order to reduce competition with state-owned telecommunications. But most literature on this topic to date concentrates on how Chinese censorship acts as a trade barrier for US companies, and focuses on Google ceasing operations in China due to strict censorship of its search engine results in 2010.[117] Google published a white paper at the time outlining how disrupting the free flow of information might violate international trade rules.[118] Internet censorship in Russia has also been characterised as a trade barrier in draft US legislation.[119]

More recently, in 2015, the Chinese government appeared to shift its censorship policy from passively blocking certain content or providers through the so-called "Great Firewall", to an actively aggressive cyber attack on an entire cloud service, the US based developer platform GitHub, named by researchers as the "Great Cannon".[120] The target appeared to be two users of GitHub, the New York Times Chinese language site, which is blocked inside China, and the anti-censorship group Greatfire.org, both of which were looking for ways to circumnavigate China's "Great Firewall" by using encrypted communications and hosting mirror pages on the US based Github platform.[121]. A Distributed Denial of Service or DDOS attack was launched on GitHub, which in turn targeted the New York Times and Greatfire.org, disabling access to those pages.

As outlined earlier in the context of data localisation, the desire to keep data within national borders, sometimes called "information sovereignty" could be applied in this context, as states wish to reduce the growth or dominance of foreign-owned companies in their domestic market. Wider global research on this topic could shed light on a practice that is both negatively impacting the free flow of data for human rights and trade.

115 Dalberg Development Advisors, Open For Business, The Economic Impact of Internet Openness (2014) p5

116 Ibid, P37

117 See: Michael A. Santoro and Wendy Goldberg, Fair trade suffers when China censors the Internet. It's not just a human rights issue, The Huffington Post (May 25 2011) and Alireza Katebi, Google vs. China- Internet Censorship, Sovereignty and Corporate Culture, The John Hopkins Carey Business School (2010)

118 Google White Paper, Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information (2010)

119 Edward J. Black, Bill to Normalise Trade With Russia Recognises Internet Censorship as Trade Barrier, The Huffington Post (September 30, 2012)

120 Citizen Lab, China's Great Cannon (April 10 2015)

121 Alex Hern, 'Great Cannon of China' turns Internet users into weapon of cyberwar, The Guardian (April 13 2015)

In Focus:
Vietnam - Decree 72

In September 2013, Vietnam's Decree 72, a controversial Internet bill, took effect. It is considered one of the world's most restrictive regulations over the Internet and contains the following provisions:

- Mobile and Internet services, including social networks, should have "at least 1 server system in Vietnam".
- Prohibits acts such as "threatening the national security, social order and safety", "sabotaging the national fraternity", "arousing animosity and among races and religions."
- Makes social networks responsible for users providing accurate personal information
- Requires that social networks should be used only to share personal information, and not news articles or information about the government.
- Imposes restrictions on what are considered "news" websites.
- Has ambiguous provisions regarding the circumstances under which social networks are obliged to hand over user's personal information to government agencies.

When the Decree was made public there was criticism from civil society groups and governments worldwide. The Freedom Online Coalition, a group of 27 governments committed to advancing freedom of expression, issued a joint statement, which referenced the direct impact of restrictive Internet laws on the economy and trade,

> *"Decree 72 risks harming Vietnam's economy by constraining the development of businesses in Vietnam, limiting innovation, and deterring foreign investment. An open and free Internet is a necessity for a fully functioning modern economy; regulations such as Decree 72 that limit openness and freedom deprive innovators and businesses of the full set of tools required to compete in today's global economy."*[122]

Decree 72 was quickly followed by Decree 174, which can impose large fines on people who may have criticised the government on social media. Freedom House reported that by 2014, Vietnam had imprisoned more bloggers than any other country in the world, apart from China.

Requirement for Internet Users to Register with the Government

Another way governments can monitor Internet users is by requiring them to register and provide their name and other personally identifiable information before they are able to buy the necessary software to access the Internet. This practice potentially leads to registered

122 Freedom Online Coalition, Joint statement on the Socialist Republic of Vietnam's Decree 72 (August 28 2013)

individuals being tracked or located, creating an infrastructure for surveillance, censorship, location and targeting of political opponents.

A number of recent examples highlight trends in this area. In May 2014 Russia enacted a new law requiring certain bloggers who had become popular, to register with the government, a measure that would give authorities a much wider ability to track who said what online. The new Russian measure specifies that any site with more than 3,000 visitors daily will be considered a "media outlet" akin to a newspaper and be responsible for the accuracy of the information published. Besides requiring registration, bloggers can no longer remain anonymous online, and organisations that provide platforms for their work, such as search engines, social networks and other forums must maintain computer records on Russian soil of all postings for the previous six months. This law gives the government the ability to identify commentators who post anonymously.[123] Russia also requires users of Public WiFi networks to register.[124] Jordan and Singapore also introduced, updated, or enforced rules requiring journalists and bloggers to register with state authorities.[125] The governments of Uzbekistan and Nigeria both passed laws that require cybercafés to keep a log of their customers, and in the case of Uzbekistan, owners must also keep records of customers' browsing histories for up to three months.[126]

Registration of mobile phones and SIM cards

Registration of mobile phones and SIM cards is a routine practice in a number of countries, such as Japan, Singapore and India. Some countries, such as South Korea, require not only that every SIM card is registered, but also every mobile phone International Mobile Station Equipment Identity (IMEI), a unique identifying number of every mobile phone.127 This has an impact on Internet users in the developing world as the Internet is mostly accessed via mobile phones (which are cheaper than laptops or other computers) and people depend on mobile phones for an array of services such as mobile banking and health care.

The main risk mandatory registration of Internet or mobile users poses to human rights is that it allows the government to track not only the communications of a person but also his or her movements, which can have serious implications to the person's security, safety, and privacy rights. Mandatory registration would require the person seeking to acquire access to mobile telecommunication to provide personal details as well as documentation that prove that the details provided are correct. This can be difficult for people who are poor, who have no fixed address, who do not earn enough to pay taxes, or who have not been registered in any national records. This places an undue burden on them. The right to seek, receive and impart information is a basic human right, and the mandatory registration places a burden that could infringe on that right.

A GSMA white paper on the implications of mandatory registration highlights a range of especially vulnerable groups that can be marginalised by the system: the homeless, those living in informal housing or remote communities, those from less well-documented groups, including those not recognised in the current census; those who are dependent on families and unable or

123 Neil MacFarqhar, Russia Quietly Tightens Reigns on Web with Bloggers Law, N.Y. Times (May 6, 2014)

124 Reuters, Russia demands Internet users show ID to access public Wifi (August 8 2014)

125Freedom House, Freedom on the Net, 2014

126 Ibid, p6

127 Usanee Mongkolporn and Asina Pornwasin, Phone users cautiously back mandatory SIM registration, The Nation South Korea (January 6 2015)

less able to leave their home to register; and those reluctant to register due to concerns over the possible violation of their privacy and/or freedom of expression (e.g. political activists, human rights defenders, trade union activists, journalists, and so on).[128]

While a number of governments have recently introduced similar requirements, others have decided against mandatory registration (e.g. the United Kingdom, Canada, the Czech Republic, Romania and New Zealand) or repealed the requirement shortly after introduction (e.g. Mexico). This is because to date no evidence has shown the effectiveness of registration in deterring terrorism or in supporting law enforcement efforts – which are usually the stated common aim of such policy measures.[129]

Studies have shown that uptake of mandatory registration actually depresses growth in mobile penetration.130 Mandatory registration can actually act as a barrier to widening the range of SIM distribution channels because it would bar sales by shops that are not owned/controlled by licensed operators or retailers. This can also undermine incomes such shop owners would have derived, adversely impacting their livelihoods.

Mandatory registration system places a cost burden on operators (through training of staff, ensuring adequate public awareness, ensuring the regular updating and accuracy of data held, and storing user data), which can potentially deter investment of innovative services and infrastructure.

Connectivity and Access

All of the above threats have two things in common: they assume Internet connectivity and access. At a Wilton Park event in November 2014, convened by IHRB with support from the Swedish Foreign Ministry[131], international participants stressed that, while the debate often gets lost in the complexities of technology and legal nuances, some countries are struggling with much more fundamental problems of access.

ICTs are an important part of the recently adopted UN Sustainable Development Goals (SDG), in particular:

> **Goal 9:** Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation which *aims to increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020.* [132] (emphasis added)

States broadly recognise the economic and social benefits of investing in and improving access in this area. Many governments plan to deliver public services online to increase efficiency and reduce costs, as outlined in a number of eGovernance proposals.[133] Other initiatives by private

128 GSMA White Paper, The Mandatory Registration of Prepaid SIM Case Users (2013) p5

129 Ibid

130 See for example, Nicola Jentzsch, Implications of Mandatory Registration of Mobile Phone Users in Africa, DIW Berlin (March 2012)

131 IHRB, Tackling Dilemmas and Dangers in the Digital Realm, Wilton Park Conference Report (November 2014)

132 UN Sustainable Development Goals (2015)

133 UN E-Government Survey (2014)

companies, such as mobile banking[134] and by NGOs, such as mHealth[135], are contributing to more prosperous and healthy citizens. Election monitoring tools[136] help to foster democracy. ICTs are increasingly recognised as a core part of disaster response. Even birth registration via SMS is set to become popular.[137]

Accessible and affordable Internet connections are the first essential step towards establishing an Internet economy. In developing countries, the costs of connectivity are often prohibitive and connections often unreliable. Users, including companies, are only able to make use of new developments, such as cloud computing and new sources of credit and financing, by relying on Internet access. As McKinsey reports:

> *"Despite the promise of the Internet as an equalising platform, the growing digital divide could leave developing economies further behind."*[138]

Digital communications have become an essential part of life in many parts of the world, and restrictions can expect to meet strong public response. When Hungary tried to impose a tax on every gigabyte of data uploaded and downloaded in 2014, over 100,000 people took to the streets in protest, throwing old computers against government buildings.[139] Neelie Kroes, the former European Commission Vice-President for the Digital Agenda described the Internet tax as a "terrible idea".[140] Following a week of protests, the plans were shelved.[141]

In addition, governments continue to reach for the communications 'off switch' in times of civil unrest or for national security reasons. While we no longer see country-wide mobile and Internet shutdowns on the scale of Egypt during the Arab Spring in 2011, disruptions may target a specific geographical area of mobile coverage, Internet access, or a specific service such as Facebook or WhatsApp, and potentially impact millions of people.

Government restrictions on access have a direct impact on freedom of expression and assembly, as well as infringing on economic, social, and cultural rights. Shutdowns can even endanger the right to life, as people are unable to access emergency services. Leading research organisation Dyn Research, which documents instances of network shutdowns worldwide, advocates for secure and diverse networks as a way to protect Internet connectivity:

> *"Outside of a few special interests, nobody profits from unstable, unreliable Internet that's subject to arbitrary political control, throttling, and shutdowns".*[142]

134 GSMA Mobile Money Programme

135 GSMA MHealth Programme

136 Jessica MacKenzie, NDI Launches Open Source DemTools for International Development, TechPresident (August 13 2014)

137 UNICEF Media Centre, Telenor and UNICEF to pilot birth registration through mobile technology (March 27 2014)

138 McKinsey Global Institute, Global Flows in a Digital Age: How Trade, Finance, People and Data Connect the World Economy (2014), p15

139Nancy Scola, Hungary's crazy-expensive Internet is driving people to throw their computers into the street, The Washington Post (October 28 2014)

140 EurActiv, Commission slams Hungary's 'Internet tax' (October 28 2014)

141 Euractive, Hungary will shelve Internet tax plan for now, Orbán says (October 31 2014)

142 Dyn Research, Syria, Venezuela, Ukraine: Internet under fire (February 26 2014)

Regular network shutdowns could damage investment in infrastructure, as companies may not see the benefit in investing in more efficient technical management systems, if they are subject to regular shutdowns. Regular shutdowns could also deter foreign direct investment.

A lack of ISP diversity at a country's borders makes networks more vulnerable to disconnection. If a country has only one or two "frontier" service providers (internationally connected domestic providers), it makes it easier for a government to disconnect services. For example, Syria, Turkmenistan, Ethiopia, Uzbekistan, Myanmar and Yemen have only one or two service providers, while the United States has more than 40 providers, making a network shutdown much more difficult to implement.[143] Ukraine has more than 200 frontier service providers, thousands of miles of fibre-optic cable connected to a variety of countries, including direct connections to major Western European exchange points. The benefit of Ukraine's connectivity was demonstrated during the Euromaiden protests in 2013, where Ukraine's Internet reportedly remained intact and fast, delivering real time information about the protests for weeks.[144]

Telecommunication companies often bear the responsibility of executing these government orders, whether to shutdown mobile networks in particular cities or regions, Internet access, or access to particular websites or messaging applications. Most countries' national laws do allow for governments to take control of communications networks during a national emergency, but the situations in which governments can exercise this power are often vague. The request process may be unclear, execution is technically complex, and there is virtually no transparency. In addition, it is still a difficult topic for companies to discuss publicly, due to the national security element.

IHRB recently completed a study of mobile network shutdowns in Pakistan, examining one particular shutdown from March 2015.[145] Experts are concerned that network shutdowns are becoming the norm in Pakistan, rather than utilised in exceptional circumstances, and considered the main strategy to curb terrorism, rather than concentrating on improving other methods of investigation. In addition, shutdowns appear to be expanding from mobile services to include Internet access, and there are proposals to ban some messaging applications such as Whatsapp and Blackberry.

Globally, shutdowns are becoming more frequent and are receiving more attention from the global community. At the time of writing, the digital rights organisation Access Now recorded 20 cases of governments shutting down Internet services in the first half 2016.[146] In July 2016, the UN passed a resolution on the protection, promotion and enjoyment of human rights on the Internet, highlighting concern regarding "measures aiming to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law".[147]

143 Ibid

144 Ibid

145 IHRB (2015) Security v Access: The impact of mobile network shutdowns. Case study: Telenor Pakistan

146 See Access Now #keepiton campaign.

147 Human Rights Council, A/HRC/32/L.20 The promotion, protection and enjoyment of human rights on the Internet (June 27 2016)

Restrictions on Cross Border Data Flows to Protect Data and Privacy

Reactions to state surveillance allegations have been particularly strong in Europe, which has extensive data protection laws. The EU General Data Protection Regulation (GDPR) recognises that, while free flow of information is essential to commerce, personal information must be protected to safeguard fundamental rights and freedoms, in particular the right to privacy.

As of 2013, 99 countries have adopted some form of data protection and privacy legislation that restricts the use and transfer of personal or other sensitive data.[148] This form of regulation is primarily intended to protect rights to information and privacy, and to prevent the misuse of personal information. Companies across industries must comply with such laws. While sound in intent, such laws can become restrictive, or they can disrupt commerce because legal frameworks across countries differ. That in turn creates compliance costs and increases unpredictability for firms. This leads to an increased regulatory cost as well for companies that need to transfer data across borders.

Businesses may experience data protection restrictions as a type of trade barrier. For example, the following types of restrictions may hinder data and hence goods and services from moving across borders:

- Outright prohibition of customer cross-border data flow to a foreign country;
- Outright prohibition of employee cross-border data flow within a group of companies to a foreign country;
- Extensive, lengthy, complex, or unpredictable procedural burdens of national data protection authority approvals of data transfer agreements; and
- Forced localisation of servers or ICT infrastructure.

Although the US and Canada share a border and are strong trading partners, the growth of cross-border data flows resulting from widespread adoption of broadband-based services in Canada and the United States has refocused attention on the possible impacts of privacy rules in two Canadian provinces, British Columbia, and Nova Scotia. These provinces mandate that personal information in the custody of a public body must be stored and accessed only in Canada unless one of a few limited exceptions applies. These laws prevent public bodies such as primary and secondary schools, universities, hospitals, government-owned utilities, and public agencies from using US services when personal information could be accessed from or stored in the United States.[149]

Some of the restrictions above are trade barriers as they bar the possibility of multi-national firms consolidating their operations across multiple territories, and taking advantage of economies of scale necessary to competitively price the services needed to enter a national market. Incumbent, typically national firms that already operate in the market can hereby benefit from entry barriers, which also limit competition in the domestic market.

Other barriers increase the transaction costs of transferring data across territories, which lead to missed business opportunities, and delay project execution and add an unnecessary increase

148 Graham Greenleaf, Local Data Privacy Laws 2013: 99 Countries and Counting,Privacy Laws & Business International Report, Issue 123, June 2013, pp10-13

149 United States Trade Representative, Foreign Trade Barriers: Canada

in administrative costs. Finally, some restrictions do not prohibit or increase the cost of cross-border data flows as such, but rather take away the entire economic incentive to compete in a national market by forcing multinational companies to invest in local IT/server infrastructure.

Governments do have legitimate interest in safeguarding the privacy of their citizens. Differing requirements, however, as to when companies can and may transfer data from one jurisdiction to the next have created trade barriers – as the free flow of much data is needed to support global services companies. The internal management of companies with employees in different jurisdictions are affected as a result. Thus, policymakers should craft solutions that allow for so called "interoperability" – creating standards that allow companies to move data – and also certify compliance in a way that allows for recognition in multiple jurisdictions.

In 2011, the leaders of the Asia-Pacific Economic Cooperation (APEC) group of Pacific Rim economies endorsed a Cross-Border Privacy Rules system based on the organisation's privacy principles.[150] Each participating economy must have its own Privacy Enforcement Authority, which in turn coordinates with an APEC-wide enforcement network. In 2012, the United States and Mexico became the first countries to participate in the system. APEC's system is scalable. Countries that are not APEC member states can opt into the system, which means that it can expand beyond APEC and, indeed, officials from APEC and Europe have developed a comparison tool for companies seeking certification under both systems. The APEC pathfinder is still in its early days and does have its critics among civil society organisations – but it is an example of a group of nations with strong trade and economic cooperation trying and address disparate privacy regimes.[151]

In its 2012 white paper on privacy, and again in its recent big-data report, the Obama Administration endorsed the idea to allow data to flow across borders by treating other countries' citizens' data largely as it would be treated in their home country when it is traveling abroad (known as interoperability). Mechanisms such as certification requirements, third-party oversight, dispute resolution, and industry-specific codes of conduct would provide necessary assurances and avoid the need for bureaucratic approval of each transaction.

In 2011, the OECD adopted Internet Policy Making Principles,[152] championed by the US as part of former Secretary of State Hillary Clinton's Internet freedom agenda. These principles recommended practices for safeguarding the free flow of data while implementing national policies on issues such as privacy, cyber-security, or consumer protection. In 2013, when the OECD updated its landmark 1981 Privacy Guidelines it directly addressed the need for further attention to the free flow of information.

The OECD Privacy Principles include "Basic Principles of International Application: Free Flow and Legitimate Restrictions." In creating these new principles, the OECD is clear that: "Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to trans-border flows of personal data that would exceed requirements for such protection." The OECD recognizes that data protection can hinder trade and economic activity.[153]

150 APEC Cross-border privacy rules system. Policies, rules and guidelines

151 Alberto Cerdo and Caroline Rosselini, Formation Flow and Trade Agreements: History and Implications for Consumers' Privacy (Consumers International May 2013), p6; see also; Greenleaf, Graham. Five years of the APEC Privacy Framework: Failure or promise? Computer Law & Security Review 25, no. 1 (2009): 28-43

152 OECD, Principles for Internet Policy Making (2014)

153 The preface to the revised 2013 OECD Privacy Principles States: "On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new

The Privacy Principles state: "Member countries should take all reasonable and appropriate steps to ensure that trans-border flows of personal data, including transit through a Member country, are uninterrupted and secure." In addition member countries are advised to "refrain from restricting trans-border flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation." More generally, the idea is to allow data transfer if the country to which it is exported observes the baseline OECD standards.[154]

The 2013 revised OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data expressly recognise appropriate measures that data controllers can implement and which, together with effective enforcement mechanisms, can qualify as sufficient safeguards. These safeguards are listed as the second scenario in which the Member countries should refrain from restricting trans-border flows.[155] The OECD Member countries considered it necessary to develop Guidelines that would help to harmonise national privacy legislation and, while upholding human rights, would at the same time prevent interruptions in international flows of data.

Annex 2 contains a summary of a recent ruling by the Court of Justice of the European Union (CJEU), in which the court invalidated a major agreement between the EU and the US, allowing for the cross border transfer of data between the US and EU member states. This ruling was meant to be a compromise that allowed for the flow of data as part of e-commerce and cross border trade, as long as US companies provided adequate privacy protections. This ruling means that what was once seen as a practical compromise between these major trading partners, to preserve data flows and protect privacy, is invalid. How this will impact the future of cross border data transfers remains to be seen.

computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance."

154 The OECD also notes that there are special cases where a country may enhance its piracy protections: "A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection."

155 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013)

III. Recommendations

Regulating technology and data flows requires subtlety and sensitivity. Technology has multiple uses, and imposing restrictions to secure a specific policy outcome can put at risk other desirable policy outcomes. Protecting one right can end up harming another. The use of blunt instruments such as bans, restrictive legislation, or disconnections can cause severe damage to human rights and affect countless lives. Restricting access to information also harms domestic innovation and people who need the Internet as an engine of economic growth.

Governments therefore need to assess, when they contemplate a restrictive measure – such as the ones highlighted in this Report – whether the perceived and intended benefits outweigh the costs, and what can be done to mitigate the harm. The costs should be assessed in terms of impacts on citizens, consumers and entrepreneurs, researchers, and anyone who needs the Internet as a vital link for their daily life and livelihood. To date, governments have not focused on all the relevant impacts in this area on trade and human rights.

As stated at the outset, there are times when state authorities will need to curb information flows for legitimate reasons. But regulators should temper their decision to ensure that their actions are not overly broad. As stakeholders critically examine the issue, questions to be considered and explored include:

- Does the proposed solution or policy restrict choice, speech, and the principles of open Internet?
- What does an action disable, and what does it enable? For example, does localisation of data (ostensibly to protect local users' privacy) end up disabling commerce, trade, and communication? Does it enable greater domestic surveillance?

With this in mind, we offer the following recommendations:

General Recommendations

- Governments should facilitate data flows. They should commit to permitting restriction-free transfer of data, subject to narrowly tailored public policy exceptions that are transparent and consistent with internationally agreed standards, and should not inhibit access by companies or individuals to information that is publicly or legally available but which is stored outside the country. They should also create interoperable standards that allow for such transfer. Reliable access to data is critical to the success of entrepreneurs, workers, and companies, and also enables the fulfilment of many human rights. Governments should ensure the safety, security and privacy of its citizens and recognise that approaches may differ between countries and across sectors.

- Governments should improve transparency and predictability and adhere to due process while regulating the digital economy. Governments should publish proposed measures in draft form and offer sufficient time and full opportunity for comment; make public requests for information or other government demands on service providers practicable to the maximum extent; and provide opportunities to contest government measures that restrict

cross border information flows. With respect to on-going trade negotiations, governments need to provide opportunity for consultation with the public.

- Governments should explore how the principles of free flow of data can be embedded in bilateral and multilateral trade agreements. Such agreements might state that parties would not introduce barriers to electronic data flows across borders unless they are necessary for security, consumer protection, or other similar public policy considerations. To the extent that such considerations are invoked, governments should be clear and transparent as to the rationale for limiting data flows.

- Government policymakers should develop strategies to determine and quantify how restrictions on cross border data flows impact trade and market access. Ministries in charge of trade and commerce should track and assess situations where businesses are impacted by restrictions on data flows. This will help policymakers understand the economic impact of various restrictions. Strategies implemented without adequate study or understanding of the full impact of specific actions may end up causing harm to trade flows as well as to human rights.

- Governments should encourage multi-stakeholder cooperation in the development of policies and rules relating to cross border data flows. These conversations should include members of the technical community, law enforcement, human rights organisations and impacted stakeholders worldwide. World Trade Organisation (WTO) member states should ask the WTO Secretariat to analyse the impact of domestic policies and laws that restrict data flows to determine if they are barriers that may be challenged in a trade dispute.

Recommendations by Issue

Data Localisation/Storage Requirements

- Governments should work to resolve emerging legal and policy issues raised by cross-border data flows, especially with respect to cloud computing. If not properly managed, new regulation in these areas could create significant non-tariff trade barriers. In particular, governments should work towards clarifying jurisdictional claims and applicable law to reduce uncertainty for businesses operating globally, and particularly so for small enterprises, which have fewer resources to navigate these complex issues.

- Governments should avoid investment mandates that require the use of local infrastructure. Government regulation of standards and technical rules can either open markets to technology or skew the market in favour of local providers or particular technologies. There is no evidence to suggest, or assure, that such local providers are superior, cheaper, or more likely to protect human rights. Governments should work to ensure fair treatment in relation to data stored out of the cloud and to standardise agreements on the treatment of data stored in the cloud between nations.

- Governments should work collectively to update and clarify mutual legal assistance obligations – flowing from existing Mutual Legal Assistance Treaties. Governments should ensure that companies and governments alike understand how and when they may request data that is housed in a different jurisdiction, due to the increase in cloud-based data

storage.[156] However, the MLA process applies only to criminal investigation, and not to intelligence gathering. Any suggestion of expanding the MLA process to intelligence agencies, given the current sensitivities around surveillance would require particular scrutiny and consultation.

Prohibition or Blocking of Certain Requirements

- Governments should recognise the importance of encryption for ecommerce and human rights. States wishing to build a digital economy should recognise that encryption is essential, not just for security of transactions but also the safety of human rights defenders. Encryption can be technologically complex, with different features and characteristics. Governments should engage a multi-stakeholder group of communications and cryptography experts as well as law enforcement and intelligence agencies, cyber security companies and human rights organisations. This should form a central part of debates on surveillance reform. If a state has criminalised the use of encryption, it should de-criminalise its use immediately.

Content Censorship through Filtering/Blocking

- The use of censorship as a trade barrier has had little attention or research, apart from the example of a few states blocking of VoIP for commercial reasons, and Chinese censorship of Google in 2010. More research on this topic could produce positive results for both human rights and economic benefit. Governments should look carefully at the reasons some states block whole services in particular.

Requirement that Internet Users Register with the Government

- Governments should not introduce registration of Internet users, mobile SIM cards or handsets for reasons of deterring terrorism as there is to date no evidence it is an effective measure. Registration appears to be enacted as a way for governments to monitor Internet and mobile users and track and locate registered individuals, creating an infrastructure for surveillance, censorship, locating and targeting of political opponents, and infringing upon freedom of expression and other rights.

- Governments should recognise evidence that registration methods depress growth of mobile penetration and could contribute to widening the digital divide by marginalising people who have no official documentation, who have no fixed address, who do not earn enough to pay taxes, or those reluctant to register due to concerns over the possible violation of their privacy and/or freedom of expression (e.g. political activists, human rights defenders, trade union activists, journalists, and so on).

156 See the Global Network Initiative (GNI) report Data Beyond Borders: Mutual Legal Assistance in the Internet age (2015) for more recommendations.

Requiring Companies to Install Filters of Other Types of Screening or Surveillance Mechanisms into Imported Hardware

- Cybersecurity is a difficult issue for any country to navigate. But imposing intrusive requirements, such as compelling companies to turn over their source code (the series of commands that create programs, a closely guarded corporate secret), submit to intrusive security testing, and building so-called 'back doors' into hardware and software erodes confidence that ultimately impacts negatively on expanded trade.

- Governments must develop cybersecurity policies, in line with World Trade Organisation (WTO) commitments, transparently and open to public consultation. In 2013, the OSCE announced it would draft a series of "confidence-building measures" to "enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs."[157] Governments should take advantage of these initiatives to ensure their cybersecurity policies do not lead to restrictions on the free flow of data.

Imposing Civil and Criminal Penalties on Intermediaries if they do not Comply with Requests to Block and Filter Content

- Some government policies in this area may have been developed with major Internet providers in mind, and with staffing and financial resources available to cope with the demands. But these policies are crippling for small companies. Some companies have opted to close down rather than deal with the burden. This risks stifling innovation and the growth of a State's home grown e-economy.

- Governments should not impose civil or criminal penalties on companies with regards to removing content, and should allow companies to appeal requests for content takedown.

Connectivity and Access

- In September 2015, the United Nations agreed to a set of 17 Sustainable Development Goals for realising fundamental rights such as health, education and livelihoods, as well as tackling gender and income inequality. ICT is a key enabler to all of these, particularly in low-income countries and ICTs are essential to achieving the new Goals. Government-ordered network shutdowns are a fundamental risk, not just to human rights organisations, national security or business operations, but also to the most fundamental of sustainable development challenges to which all states are party.

- Governments should never require companies to shutdown access to communications for the entire country. One area to explore is whether companies could include instances where they have been ordered to wholly or partially shut down a network, or where they have been asked to block access to a particular service, in their transparency reporting. The laws in

157 OSCE Decision No. 1106 Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies (December 3 2013)

some countries prevent companies from even revealing this information, and some companies believe the onus should be on governments, not companies, to publish this information.

- Governments should clarify and limit the law on telecommunications network shutdowns, and commit to never shutting down the Internet, in line with international standards. A suspension of telecommunication services (mobile and landline) must be prescribed by law and only be invoked if there is a real and imminent threat to national security or a national emergency. There must be a clear and transparent process around who is authorised to make a shutdown request. Shutdowns should be limited in geography, scope and duration, and should be publicly reported after the fact.

- Governments should not prevent telecommunication companies from reporting on network shutdowns after the fact.

Restrictions on Cross Border Data Flows as Part of Data Protection

- Governments do have legitimate interest in safeguarding the privacy of their citizens. Privacy protections are important. Differing requirements as to when companies can and may transfer data from one jurisdiction to the next have created trade barriers – as the free flow of much data is needed to support global services companies, and the internal management of companies with employees in different jurisdictions are affected as a result. Thus, policymakers should develop policies that allow for so called "interoperability" – creating standards that permit companies to move data – and also certify compliance in a way that is recognised in multiple jurisdictions.

- Governments could explore cross-border data sharing models, such as experimenting with data sharing on certain services.

Annex 1. Mutual Legal Assistance Reform: The Way Forward?

In the legal case brought against the US Government regarding a US warrant served on a US company to hand over data held on servers in Ireland, Microsoft argues that for data held overseas, the US government should strengthen and abide by its mutual legal assistance treaties, or MLATs.[158] These are agreements between countries or regions to share information relating to criminal investigations in one of those countries. This process is in need of reform, not least because of the huge rise in requests, but also because the process relies on physical documents manually being sent back and forth rather than electronically.[159] Many stakeholders would like to see the reform and strengthening of the MLAT process as a solution to the issues relating to cross-border data, or as one expert describes it, "information sovereignty".[160] Microsoft's legal counsel has even suggested a new international convention on government access to data should be considered to supplement existing MLAT rules.[161]

A 2015 Global Network Initiative (GNI) report called *Data Beyond Borders: Mutual Legal Assistance in the Internet Era*[162] highlighted that an inadequate MLA regime means governments resort to other tactics to obtain information, such as demanding data localisation, applying national laws extraterritorially, or placing the onus on technology companies to volunteer information. The report lists key requirements for MLA reform, and sets out recommendations for improving the request process and strengthening the treaties. Recommendations include the following:

- Requests should be submitted electronically, in a uniform request format, and States should create an internal tracking system for managing requests.
- All requests must explain the legal justification and there should be a time limit on responses.
- The report also sets out recommendations for increased transparency, efficiency and allow for scalability, as the amount of MLA requests is expected to grow over the years.

The report also recommends that the reforms should be designed to ensure protection of human rights as a priority. Reforming this process could be one avenue to ensure the issue of "information sovereignty" does not cripple the free flow of information. It is one that any company involved in collecting and storing user data should take interest in. As the GNI report states:

> *"All companies engaged in communications and e-commerce have a legitimate interest in a clear and predictable legal framework for managing government access to customer data-one that adapts to the ways of modern business."*

158 See https://mlat.info/

159 Hill, Jonah Force, Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for US Policy Makers. Berkman Center Research Paper (2012)

160 Evgeny Morozov, Who is the true enemy of Internet freedom- China, Russia of the US? The Guardian (January 4 2015)

161 Microsoft Corporate Blog, Time for an international convention on government access to data (January 20 2014)

162 Global Network Initiative (GNI), Data Beyond Borders: Mutual Legal Assistance in the Internet age (2015)

The UK's independent reviewer of terrorism legislation, David Anderson, recently published a report echoing calls for strengthening the MLAT system[163] and presented recommendations,

> *"It is not recommended that service providers wishing to offer services in the UK should be required to have a license, or that they should be required to store data in the UK. But in order to address deficiencies in access to material from overseas service providers, the Government should:*
>
> *(a) seek the cooperation of overseas service providers, including by explaining so far as possible the nature of the threat, how requests are authorised and overseen, and the steps that are taken to ensure that they are necessary and proportionate;*
>
> *(b) seek the improvement and abbreviation of MLAT procedures, in particular with the US Department of Justice and the Irish authorities; and*
>
> *(c) take a lead in developing and negotiating a new international framework for data-sharing among like-minded democratic nations."*[164]

In September 2014, Sir Nigel Sheinwald was appointed as the UK Special Envoy on Intelligence and Law Enforcement Data Sharing. In June 2015, he published a summary of his recommendations[165], which also advocate for MLAT reform, and proposed the development of a new international framework for data sharing.

163 Ibid p208

164 Ibid p289

165 Summary of the work of the Prime Minister's Special Envoy on intelligence and law enforcement data sharing- Sir Nigel Sheinwald (2014)

Annex 2. The Loss of the US-EU "Safe Harbour" Agreement

The European Union is known for being rigorous on data protection issues. Companies operating in the EU are not allowed to send personal data to countries outside the EU unless there is a guarantee that the data will be adequately protected. Since 2000, the United States and EU have relied on a negotiated "Safe Harbour" agreement used by around 4,500 companies[166], whereby US companies are allowed to store and engage in cross border transfer of data on EU citizens, as long as they adhere to the Safe Harbour Principles, and agree to provide adequate privacy protection.

In the wake of the mass surveillance revelations in 2013, Austrian privacy advocate Max Schrems brought a case against Facebook in Ireland, where Facebook's European operations are based, arguing that the company was breaching his rights as an EU citizen, as US laws do not protect non-US citizens from surveillance by US intelligence agencies. The case was referred to the Court of Justice of the European Union (CJEU), which ruled in October 2015 that the Safe Harbour agreement is invalid, because it violates European citizens' privacy by exposing their personal data to US government surveillance that would be illegal in the EU.[167]

Some of the main points of the ruling included:[168]

- Individual European countries can now set their own regulation for US companies' handling of citizens' data, vastly complicating the regulatory environment in Europe.
- Countries can choose to suspend the transfer of data to the US — forcing companies to host user data exclusively within the country.
- The Irish data protection authority will now examine whether Facebook offered European users adequate data protections, and it may order the suspension of Facebook's transfer of data from Europe to the US if so."

While it can be argued this is a victory for privacy advocates and the next step in surveillance reform, it can have implications for business relying on transatlantic data transfers. The decision did not appear to order an immediate end to personal data transfers and it was unlikely to stop data flows immediately, but it raised compliance issues for US firms handing European citizen's data.

Oversight of Safe Harbour was delegated to the Federal Trade Commission (FTC) and the Department of Commerce with minimal oversight by the European Commission. After being in effect for nearly 15 years, Safe Harbour compliance by US companies was rarely questioned or enforced by the FTC or the Department of Commerce. Many viewed Safe Harbour as merely a "promise" of compliance by the US. The lack of attention and oversight by US authorities, along

166 Natalia Drozdiak and Sam Schechner, EU court says data-transfer pact with US violates privacy, The Wall Street Journal (October 6 2015)

167 Henry Farrell and Abraham Newmn, This privacy activist has just won an enormous victory against US surveillance. Here's how. The Washington Post (October 6 2015)

168 James Cook and Rob Price, Europe's highest court just rejected the 'safe harbor' agreement used by American companies, Business Insider UK (October 6 2015)

with revelations regarding US government surveillance, eventually led to the recent case in which the CJEU invalidated the Safe Harbour.

According to reports, large US companies such as Facebook, Google, and Apple, which already have data centres based in the EU, may have to re-engineer their systems to keep US and EU data entirely separate, which will require significant resources.[169] The Safe Harbour agreement was already being renegotiated, albeit with an unclear timetable, which may have spurred large companies to start establishing European data centres anyway. But smaller companies may find it prohibitively expensive to set up data centres in Europe, or to reengineer their operations in the way that bigger companies may be able to.[170]

When previously companies had to self-certify that they were complying with Safe Harbour principles, they would have to prove they are complying with EU data protection laws, or risk being investigated by EU data protection regulators.[171] EU law provides for other ways to transfer personal data legally. Among them are so-called model contract clauses, which use language approved by European officials. A spokeswoman for Amazon said in a statement that Amazon Web Services, the retailer's cloud-computing division, had already obtained approval from the EU for its model contracts.[172]

By early 2016, a replacement agreement was under negotiation, and the draft text of the "Privacy Shield" agreement was published. Some experts believe that the new deal significantly strengthens European's privacy rights and improves privacy protection of US citizens.[173] But privacy campaigners are dissatisfied with continued self certification provisions, a lack of enforcement mechanisms and a failure to address the wider issue of reforming surveillance laws in the EU and US, which allows data collection and retention in bulk.[174] Max Schrems suggested that the Privacy Shield does not address the issues that brought about the invalidation of Safe Harbour in the first place.[175]

At the time of writing, the agreement was in the last stages of being approved and adopted by national representatives of EU member state governments. But some commentators predict that the agreement will end up before the CJEU again before long.[176]

169 Henry Farrell and Abraham Newmn, This privacy activist has just won an enormous victory against US surveillance. Here's how. The Washington Post (October 6 2015)

170 Natalia Drozdiak and Sam Schechner, EU court says data-transfer pact with US violates privacy, The Wall Street Journal (October 6 2015)

171 Ibid

172 Ibid

173 Julie Brill, Privacy Shield is the right replacement for Safe Harbour, EurActiv.com (July 7 2016)

174 Access Now, Civil society coalition: "Privacy Shield manifestly fails to meet standards set by EU law" (March 16 2016)

175 Rachel Stern, Max Schrems: "Privacy Shield won't protect Europeans from surveillance" Passcode (May 6 2016)

176 Jennifer Baker, Privacy Shield to be dragged across finish line- Sources, Arts Technica UK (July 7 2016)

No Trade Off:

How the Free Flow of Data Enhances Trade and Human Rights

Background

In recent years, governments have deployed several legislative and regulatory measures aimed at prohibiting the use of certain technologies or applications, blocking website content, and requiring that data reside on local servers - all as a means of controlling and impeding information flows. These restrictions are imposed, at times, with a view to protecting national security or national interests. Such restrictions may curb privacy as well as other human rights, and may limit legitimate economic activity, including cross border trade.

Message

Cross border data flows are integral to international trade transactions, which increasingly rely on information exchange, electronic payments, and cloud storage. Restrictions on the free flow of information not only hinder economic growth, they can also lead to adverse human rights impacts.

Find Out More

This report provides an overview of the connections between trade and human rights and the importance of data flows in this context, as well as current threats and obstacles to cross border trade and the free flow of information.

It examines six areas in which government-imposed restrictions on the free flow of information could impact negatively on trade and human rights, and provides recommendations to governments legislating in often sensitive areas including:

- Data localisation
- Encryption
- Content censorship through filtering/blocking
- User registration requirements
- Connectivity and access
- Restrictions on cross border data flows

IHRB

Institute for Human Rights and Business
34b York Way
London N1 9AB
UK

Phone: (+44) 203-411-4333
Email: info@ihrb.org