Global Digital Futures Policy Forum 2016: Issues Brief

Panel 2: National Data Governance in a Global Economy

By Anupam Chander

Introduction

Global data flows are the lifeblood of the global economy today and of the technologies of the future. Yet, the regulation of how data is to be handled remains largely the province of national laws. How we resolve the dilemmas of global flows within a nation-state structure will impact the digital economy, free expression, privacy, security, consumer protection, and taxation. Just as we once built an architecture for cross-border flow of goods, we need to build an architecture for cross-border flow of information.

Problem Statement

In the absence of, at minimum, a *modus vivendi* for global data flows, the World Wide Web may increasingly tear apart, and the global Internet may disintegrate into national or regional 'Splinternets.'

Issues

Global Data Flows Are Crucial to Innovation

Many of the most promising technologies and economic innovations rely on global data flows. Consider the following ten recent developments:

1. **The Internet of Things.** Devices like an Apple Watch or a Samsung Smart TV — or even a John Deere or Komatsu heavy machine — depend on the flow of information across national borders to gather and process data.
2. **App Economy.** Individuals and small companies can now build applications and leverage global marketing, distribution, and payments networks to sell their products and services to the nearly 2 billion smartphone users across the world.
3. **Outsourcing of Services.** The ability to outsource business processes and information technology services depends on the cross-border flow of information.
4. **E-commerce.** Companies like Alibaba and eBay depend on global information flows to enable people to sell to, and buy from, global markets.
5. **Cloud computing.** Cloud computing depends on the transfer of large volumes of information, often across borders, to server farms typically located based on network efficiencies, security, and costs. Robots, for example, increasingly depend on cloud-based information storage and processing.
6. **Big data.** Data sets can be larger if they include people across borders; analytics are often performed using tools and companies located in foreign jurisdictions.
7. **Digital products and streaming services.** Digital music and video services, from Apple, Netflix, Spotify, and others, increasingly allow customers across the world to download

or stream audiovisual content.

8. **Social media and websites generally.** Social media, and the Web generally, implicate significant information sharing across borders.
9. **The sharing economy**. AirBnB, Uber, and the like allow one to share one's resources, often for a price, with people from anywhere in the world.
10. **Crowdfunding**. People planning new projects can now raise funding from supporters across the world.

Rules that make it difficult to move data across borders will complicate and even at times make impossible efforts to offer such innovations. For example, if companies rolling out Internet-enabled devices have to create or purchase separate data infrastructures for each country in which they operate, the costs of providing many such devices may prove prohibitive. Companies like AirBnB, Uber and Upwork depend on individuals across the world sharing information across national borders. Finally, rules that prevent information from leaving home except in difficult to obtain circumstances can effectively bar foreign service providers offering back office outsourcing from processing information (a result that trade protectionists favor).

The Rise of Internet Border Controls: From Censorship to Data Localization

Efforts by national governments to assert control over global data flows trace back at least to the turn of the Millennium. A French court ordered Yahoo! to prevent Nazi material from being made available within France. Yahoo! protested that they should be governed by the liberal free speech codes of their American home, but the French court was unpersuaded, and Yahoo! voluntarily complied by removing the material from its services everywhere. A more notorious application of governmental efforts to control information can be found in the so-called Great Firewall of China, which enlists Internet companies in censoring material within the country. Recently, France's privacy regulator has penalized Google for failing to remove search results subject to the "right to be forgotten" from sites outside France, not just from results accessible in France as Google was prepared to do.

The French Yahoo! decision and the Great Firewall of China represent what we might describe as the first generation of Internet border controls, that is, efforts to control information coming *into* a country. "**Data localization**" is the name for a less familiar but increasingly popular new kind of Internet border control. This second generation of Internet border controls seeks to keep information from going *out* of a country. Governments seek data localization on a variety of grounds, from data protection to outright protectionism.

Many governments have increasingly sought "**data sovereignty**," often seeking both to control data within their countries and to limit the flows of data outside their countries. The globalization of data raises issues that the globalization of goods did not, because data often contains very personal information, for example about our searches, our likes, our friends, our finances, and our health. It is easy to use the sensitivity of data to bar foreign service providers by requiring that data be stored or processed by local providers. Assertions of data sovereignty often coincide with a general industrial plan to grow a local set of Internet services to displace the largely American leaders (including Google, Apple, Facebook, and Amazon, or "GAFA" as

they are sometimes labeled in Europe). Experience with trade in goods, however, tells us that it is possible to meet varying national safety standards even when importing goods from abroad.

Figure 1. Internet Border Controls

	First Generation	**Second Generation**
Type of control	Censorship	Data Localization
Stated Goals	Prevent unwanted information from entering country for social or political purposes	Prevent information from leaving country to (1) protect privacy (though privacy can be protected even when information is processed abroad); (2) assist local law enforcement, surveillance & control; (3) promote local enterprise
Examples	Great Firewall of China	Russian data localization

Protecting Privacy and Avoiding Foreign Surveillance

Last year, the European Court of Justice took up an Austrian law student's challenge to Facebook's processing of his personal information. In *Schrems v. Irish Data Protection Commissioner*, the court concluded that United States surveillance practices meant that European data could no longer be processed in the United States under an existing Safe Harbor agreement. In response the United States has agreed to added protections against mass surveillance for Europeans under a "Privacy Shield" arrangement, including a right under a new United States Judicial Redress Act to sue the U.S. government for mishandling their data. Some in Europe have criticized the new arrangement as containing inadequate guarantees.

The case against Facebook recalls two other cases in which American companies have been asked to assist U.S. law enforcement. In 2013, a US. judge directed Microsoft to turn over user information stored on its Irish servers, but Microsoft has challenged the order, earning the support of the Irish government. Most prominently, in a domestic case with international implications, Apple fought the U.S. government's initial efforts to compel it to assist in defeating a security feature on its iPhone, in part because complying would empower other governments to demand Apple's assistance as well.

Because both Europe and the United States recognize the importance of cross-Atlantic data flows to the economies of both regions, a new arrangement permitting transfer must be found to allow information to flow across the Atlantic. As it stands now, companies and individuals continue to transfer information because of necessity, but lack any assurance that such transfers will not subject them to liability. As the European Union (EU) implements the new General Data Protection Regulation (replacing the 1995 Data Protection Directive), liability

under EU law becomes ever more alarming, potentially subjecting a company to fines up to four percent of the company's annual global turnover.

Conclusion: Charting a Path Forward in Cyberspace

If we are to gain the enormous benefits from information exchange made possible by the Internet, we will need to engage in a series of reforms. These may include:

- *Surveillance Reform*. Need for respecting dignity of foreigners abroad; recognize that International Covenant on Civil and Political Rights (ICCPR) obligations apply to a government's actions not just at home, but also with respect to foreigners abroad. The US EU Privacy Shield provides some assurance that Europeans will not be subject to mass surveillance by U.S. authorities, including actionable guarantees of freedom from mass surveillance under the Judicial Redress Act. Thus far, it is unclear whether citizens of foreign countries outside Europe might benefit from similar guarantees of freedom from mass surveillance.

- *Privacy protections*. Governments need to ensure data protection, so that privacy and security are upheld regardless of where data flows. Here there a number of competing models, including the European Union's General Data Protection Regulation (an omnibus consent based approach to all processing of personal information regardless of entity) or the United States sectoral privacy law (focused on certain categories of sensitive information held by industry professionals) coupled with privacy promises enforced by the Federal Trade Commission and class action lawyers.

- *Free Trade Commitments*. Commit governments to permit data to flow across the world and services to be performed from abroad, unless legitimate interests such as privacy require otherwise. If it is ratified, the Trans-Pacific Partnership agreement between a dozen Pacific rim nations would require governments to permit cross-border data flows unless justified by a "legitimate public policy objective." It is unclear whether the Transatlantic Trade and Investment Partnership (TTIP) being negotiated between the United States and Europe will subject European crossborder data flow restrictions to any trade disciplines. Finally, the Trade in Services Agreement (TiSA) being negotiated now between a large number of developing and developed nations, including the United States and nations of Europe, seems likely to include provisions favoring crossborder data flows.

- *Crossborder Government Access to Data*. Reform of the cumbersome Mutual Legal Assistance Treaty process is needed, but any reform must respect human rights limits on government access. The current process is flawed in multiple respects. As a map by Access Now makes clear (see https://mlat.info/), not every country has a law enforcement information sharing agreement with every other country. A United States statute from 1986, the Stored Communications Act, prohibits Internet companies subject to the law from sharing information with foreign governments, permitting sharing only with "governmental entities" (defined as "a department or agency of the United States or any State or political subdivision thereof"). Finally, even when a law enforcement agency

seeks information through the MLAT process, compliance is painfully slow. Governments will need to work in multiple forums to improve human rights-protective systems of government access to information stored across borders. Because security information held abroad will often be held by corporations, corporations too must pay increasing attention to what rules they follow in providing access to foreign service providers.

- *Dispute Resolution*. Encourage the development of Internet-based crossborder dispute resolution systems. Existing trade agreements and even the "twenty-first century" agreements being negotiated now lack low cost mechanisms accessible to consumers and businesses to resolve disputes. Companies like eBay and PayPal have created their own global dispute resolution systems, and it seems likely that more private efforts to create such Internet based mechanisms will emerge.