WORLD BANK GROUP
Macroeconomics, Trade & Investment

December 2018 · Number 3

Macroeconomics, Trade & Investment
MTI Practice Notes

Trade, Cross-Border Data, and the Next Regulatory Frontier:
Law enforcement and data localization requirements[1]

Martín Molinuevo and Simon Gaillard

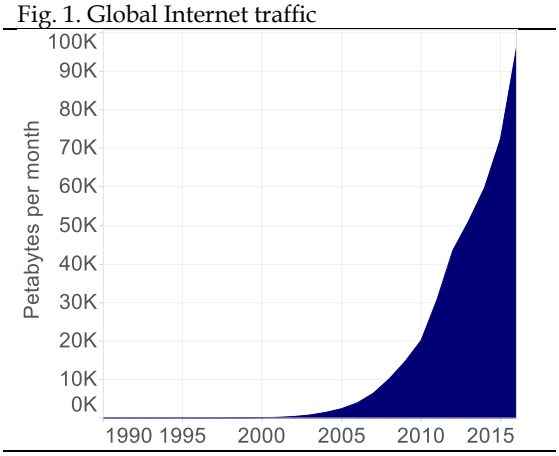
Introduction

Policy-makers and regulators are striving to tackle the challenges brought by the recent exponential growth of cross-border data. One sensitive policy concern is how to ensure access to data by law enforcement, which has led countries to impose data localization requirements or other heavy-handed responses. Existing regulatory tools are poorly equipped to address these challenges of the digital age. Innovative regulatory solutions, focused on cooperation and the recognition that firms may be required to produce data regardless its physical location, can help bring a balance between free data flows and the need to ensure effective law enforcement.

What do digital communications mean for international trade?

Cross-border data flows are becoming the defining hallmark of international trade in the 21st century. While trade in goods has slowed in the last decade, cross-border flows of data have surge dramatically (MGI 2016). Cross-border data multiplied more than 100 times, between 2005 and 2017, and this number is expected to nearly quadruple by 2021[2].

Fig. 1. Global Internet traffic



Source: Cisco Systems, reproduced by Wikipedia

To visualize this exponential growth of internet traffic (Figure 1) that all global data communications were in the format of an MP3 song (the music you can listen in your phone or mobile device). To listen to all the data transmitted globally in the year 1990, you would have needed about 25 years –about the time span of one generation. Today, to listen to one single minute worth of data flows will require the MP3 song to play for some 4,600 years. Or the entire human written history. This boom of digital communications has equally impressive economic implications: some studies estimate that data flows have contributed USD 7.8 trillion to global economic activity during the last decade, amounting to 10% of global GDP (MGI 2016).

[1] This note was prepared by Simon Gaillard (consultant) and Martín Molinuevo (Senior Counsel, MTI). The authors are grateful to Caroline Freund (Director, MTI), David Satola (Lead Counsel, LEG), Anupam Chander (Professor, Georgetown University), Michael Ferrantino (Lead Economist, MTI), and Yanina Budkin (Senior Communications Officer, MTI) for their insightful comments and suggestions.

[2] TheAtlas.com https://www.theatlas.com/charts/rJvTuVL0e.

This colossal global exchange of information has novel implications for business and for public policy. For businesses, cloud computing allows firms to organize and structure their operations more efficiently, boosting outsourcing services, and creating new opportunities for firms to join, and expand, global value chains. In the realm of policy-making, cross-border data flows bring a series of unprecedented situations to the attention of the regulator –situations that include key public policy concerns such as national security, individual privacy, economic development, and law enforcement. All these policy matters present specific challenges and require dedicated attention. This note focuses on the relationship between cross-border data and law enforcement and highlights possible alternatives to balance these policy goals.[3]

What challenges do cross-border data flows bring to regulators?

Countries are adopting diverse regulatory responses to the increasing volumes of cross-border data. Among them, bans on transferring data abroad or the obligations to store data in servers physically located in the country ("data localization requirements") have attracted particular attention. Some studies have focused on the costs that such measures entail for the economy –predicting alarming declines in GDP, foreign investments (Bauer et al, 2015 [4]), international trade (Kommerskollegium, 2014[5]) and productivity (van der Marel et al, 2016[6]), and concluding that "any gains stemming from data localization are too small to outweigh losses in terms of welfare and output in the general economy" (Bauer et al, 2015). Yet few studies (and no quantitative analysis) consider the rationale behind such measures, and whether data localization requirements may in fact be an adequate response to legitimate policy concerns. Chander and Lê (2015)[7] review data localization regulations around the world and judge that alternative measures exist in all cases to achieve the purported policy goals.

One of the policy goals often prompting data localization requirements is the need to ensure the access to data by law enforcement. [8] Whereas other rules on data governance, such as on privacy protection, are desirable as a tool to increase trust in the digital markets, disciplines on data governance and its relationship with law enforcement provide courts with effective regulatory tools to carry out their law enforcement duty in the era of digital communications, while at the same time ensuring that online services are not unnecessarily burdened in that process. The tension arises when law enforcement agencies need to access data that is stored in a foreign jurisdiction and lack specific tools to compel the online provider to produce the data. In that case, courts may fail to obtain the necessary information –potentially leaving a case unsolved as a result- or may resort to draconian measures that unnecessarily burden services providers and impact consumers –hence hampering the global digital market.

How can cross-border data flows hamper law enforcement – and vice versa?

Some recent high-profile cases illustrate the challenge that global data flows can bring to law enforcement: The recent case *United States*

[3] In particular, the discussion focuses on the ability of ordinary courts, including in civil and criminal cases, to access data retained by online services providers. This note does not discuss the ability of intelligence services or other law enforcement organizations, such as specialized anti-terrorism agencies, to retrieve such data covertly, often without the knowledge of the online service provider itself.

[4] Bauer, M., H. Lee-Makiyama and E. van der Marel (2014), The Costs of Data Localisation, ECIPE, 2014.

[5] Kommerskollegium, "No Transfer, No Trade - The Importance of Cross-Border Data Transfers for Companies Based in Sweden", National Board of Trade of Sweden, 2014.

[6] van der Marel, E., H. Lee-Makiyama, M. Bauer and B. Verschelde (2016) "A Methodology to Estimate the Costs of Data Regulation", International Economics, Vol. 146, Issue 2, pages 12-39

[7] Chander, Anupam and Le, Uyen P., Data Nationalism (March 13, 2015). Emory Law Journal, Vol. 64, No. 3, 2015. Available at SSRN: https://ssrn.com/abstract=2577947

[8] Chander, Anupam and Le, Uyen P., Data Nationalism (March 13, 2015). Emory Law Journal, Vol. 64, No. 3, 2015. Available at SSRN: https://ssrn.com/abstract=2577947

vs. Microsoft Corp[9] demonstrated the linkages between cross-border data flows and the ability of courts to investigate and legitimately persecute unlawful conduct. In this case, US federal prosecutors investigating a drug trafficking case in 2013 served a warrant to Microsoft Co. to provide the emails of an individual. Microsoft handed data stored on U.S. servers, the person's address book, but didn't deliver the actual content of the individual's emails, arguing that they were stored in a Microsoft data center in Dublin, Ireland, and the warrant by US authorities did not have extraterritorial application. U.S. prosecutors argued that, because the facts of the case took place in the United States and Microsoft is a U.S.-based company [10], producing a copy of such information does not entail extraterritorial effects of the warrant, but a mere compliance with a warrant by a U.S. court. The case was brought to the United States Supreme Court but ended without a ruling due to the passage of the new Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") on March 23, 2018. This law allows federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil.

The circumstances of this case raise substantial questions related to the regulation of cross-border data flows and law enforcement procedures. With no data localization requirements in the U.S., companies like Microsoft, which has over 100 data centers in 40 countries, could potentially move data swiftly for business purposes and thus hamper law enforcement work.[11] If firms are free to transfer and store data in any physical location of their choosing, how can law enforcement agencies obtain access to such information? How can policy-makers ensure that data regarding offenses occurring within their jurisdiction, by their own nationals, being stored by a domestic company remains reachable?

Courts from developing countries have also faced similar challenges in retrieving data from foreign jurisdictions, resorting at times to heavy-handed measures to overcome them. Brazilian courts have come in multiple occasions to stand-offs with online services who refused to produce data. An early case in 2006 entailed an order from a federal judge issued to Orkut, a social media platform owned by Google and one of Brazil's most popular websites at the time, to provide details on over twenty Brazilian nationals alleged to be using the social platform for spreading child pornography and selling drugs. After an initial refusal by Orkut on the argument that the information was not stored in Brazil, but in Google's servers in the U.S. –for which the judge imposed a fine of USD 23,000 a day-, Google agreed to cooperate with the Brazilian judge's request and hand over the information.[12] A similar case occurred in 2016,

[9] Matsakis, Louise, "Microsoft Supreme Court case has bign implications for data", Wired, February 27, 2018, https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/

[10] Given the confidentiality of the procedures, it remains undisclosed the nationality of the individual, or whether the emails were generated within the United States, or the reasons why the account content was physically stored in Ireland. This latter fact may relate to the individual having indicated Ireland as its country of citizenship or residency, or simply to a business decision by the Microsoft. On the facts of the case, see Harvard Law Review, "Microsoft Corp. v. United States", 130 Harv. L. Rev. 769, December 6m 2016, https://harvardlawreview.org/2016/12/microsoft-corp-v-united-states/ and Lawreview, "Microsoft Corp. v. United States", 102 Minnesota Law Review 6, February 23 2017, http://www.minnesotalawreview.org/2017/02/microsoft-corp-v-united-states/

[11] Barnes, Robert, "Supreme Court to consider major digital privacy case on Microsoft email storage", Washington Post, October 16, 2017, https://www.washingtonpost.com/politics/courts_law/supreme-court-to-consider-major-digital-privacy-case-on-microsoft-email-storage/2017/10/16/b1e74936-b278-11e7-be94-fabb0f1e9ffb_story.html?utm_term=.85a60c2da3d0

[12] Nakashima, Ellen, " Google to Give Data To Brazilian Court", Washington Post, September 2, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/09/01/AR2006090100608.html; Morphy, Erika, "Google to Comply With Brazilian Court Order", TechNewsWorld, September 5, 2006, https://www.technewsworld.com/story/52830.html; and Wikipedia, "Orkut", https://en.wikipedia.org/wiki/Orkut#Brazil. Eventually, Orkut went further in the cooperation with Brazilian authorities, granting the federal

in an judicial attempt to retrieve data from an encrypted end-to-end chat mobile app (WhatsApp). [13] Faced with WhatsApp non-compliance, the judge ordered first the arrest of Facebook's (WhatsApp parent company) executive vice-president (released one day later by order of the Court of Appeals, who deemed the arrest arbitrary and unjustified)[14] and later to block WhatsApp services in Brazil altogether for 72 hours (overturned on appeal only hours later)[15]. Another similar, but unrelated case involving WhatsApp in 2016 entailed the freezing of Facebook's bank accounts in Brazil for over US$ 6 million in fines, as a result of months of non-compliance with a court order issued in an investigation of an alleged international cocaine smuggling ring.[16]

What are the existing tools for cooperation in law enforcement in the digital age?

Mutual Legal Assistance Treaties (MLATs) are to date the main tool for international cooperation in law enforcement. MLATs are traditionally oriented to fulfilling criminal and public investigation procedures like obtaining testimony of witness located abroad, executing search warrants in foreign jurisdictions, or obtaining records of financial institutions abroad.

However, MLATs are poorly suited to address these challenges of the digital age. MLATs can be cumbersome and time-consuming, not only due to the rigorous legal requirements that they entail, but also due to the limited resources often available for this kind of international cooperation.[17] They are designed for courts to reach assets, companies, and people, that are less mobile than the fleeting storage of bytes. Further, if the data controllers are free to move personal data around at will, and could disregard injunctions to produce required information by legitimate authorities, nothing prevents businesses from storing data in specific jurisdictions that are unresponsive to judicial cooperation, hence effectively providing a safe haven from legal prosecution. Unscrupulous firms could build a business model around such practices.

What other solutions can help law enforcement while fostering seamless cross-border data flows?

Policy makers who wish to support global trade and investment flows with an open cross-border data regime should be able to do so, without sacrificing their domestic law enforcement capacity. Data localization requirements, while potentially effective to ensure access to data by law enforcement, do entail costs that can hamper businesses. Innovative regulatory solutions should reconcile these policy objectives.

- Legislation may grant domestic courts the ability to request its citizens and firms to produce data regardless of its physical location, overcoming the need for data

police direct access to Orkut's accounts and to the ability to monitor and even to delete users accounts in real time, without the need for a judicial order (Pagnan, Rogério, "Orkut dá à PF "atalho" para barrar páginas", Folha de S.Paulo, November 28, 2006. https://www1.folha.uol.com.br/folha/informatica/ult124u21063.shtml).

[13] Wikipedia, "Whatsapp", https://en.wikipedia.org/wiki/WhatsApp#Brazil

[14] G1 Sao Paulo, "'Felizes', diz Facebook sobre soltura de vice-presidente preso em SP", O Globo, February 2, 2016, http://g1.globo.com/sao-paulo/noticia/2016/03/felizes-diz-facebook-sobre-soltura-de-vice-presidente-preso-em-sp.html

[15] G1 Sao Paulo, "WhatsApp: Justiça do RJ manda bloquear aplicativo em todo o Brasil", O Globo, July 19, 2016, http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-deve-ser-bloqueado-decide-justica-do-rio.html?utm_source=push&utm_medium=app&utm_campaign=pushg1; Farivar, Cyrus, "Brazilian appellate judge rescinds WhatsApp block", arsTechnica, May 3, 201, https://arstechnica.com/tech-policy/2016/05/brazilian-judge-blocks-whatsapp-for-72-hours-but-it-still-works-over-vpn-wi-fi/; BBC News, "WhatsApp in Brazil back in action after suspension", BBC, July 20, 2016, https://www.bbc.com/news/world-latin-america-36836674.

[16] Commuter, ""Brazil court blocks Facebook funds over Whatsapp dispute: Report", Commuter, n/d, https://worldcommuter.com/brazil-court-blocks-facebook-funds-whatsapp-dispute-report/.

[17] Force Hill, Jonah, "Problematic Alternatives: MLAT Reform for the Digital Age", Harvard National Security Journal, January 28, 2015, http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/.

localization requirements. The recently approved CLOUD Act [18] distinguishes between data from Americans and non-Americans held abroad on servers of American companies. [19] This legislation allows for the retrieval of data by American citizens held abroad thus bypassing MLATs, making it mandatory for firms to comply with such court order. Conversely, the CLOUD Act also permits foreign governments that have entered into executive agreements with the United States government to obtain information from U.S.-based internet companies.

- Other solutions may focus on strengthening cooperation between law enforcement agencies and/or between national data protection authorities. Stronger cooperation could focus on expedited consideration and implementation of the request from foreign authorities, while ensuring that privacy concerns of citizens and residents remain well protected. Such regulatory agency cooperation is hardly a novelty. Competition authorities, across the Atlantic and with many other countries, have established strong collaboration frameworks in cases related to transnational anti-competitive behaviors. Specific to cybercrime, "24/7 Networks" seek to ensure points of contact in law enforcement agencies in different countries that can respond in real time and jointly to cyberattacks and other cyber-crimes.[20]

- Trade agreements could support international rules on the interplay between data flows and law enforcement. By recognizing that court orders may, under certain conditions, reach online firms that are not established in the court's jurisdiction, they could help prevent burdensome punitive measures on cross-border providers that unnecessarily disrupt the broader digital market. To that end, a softly worded provision, similar to existing provisions on e-commerce cooperation in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) or the EU – Canada Comprehensive Economic and Trade Agreement (CETA), could promote greater collaboration between the parties in this field, or even serve as legal grounds for courts to request data from non-established firms.

- Finally, guidelines in the form of rules of conduct for firms responsible for data storage and processing could also provide a valuable instrument to support domestic law enforcement efforts. Firms established in the country, or firms located abroad who offer services in that country would need to comply with such rules to facilitate law enforcement, much like the Privacy Shield between the US and EU provide a framework for compliance with privacy regulations.

The interaction between cross-border data flows and law enforcement offers an example of the challenges that new technologies can bring to policy making. New forms of information sharing, and its sheer volume, unthinkable only one generation ago, are creating formidable opportunities for business, spurring economic growth. These interactions, however, can affect sensitive public policies, such as the need to protect privacy, establish a conducive environment for trade and investment, or ensuring safety and security. These policy-making challenges are only at their initial phases, and warrant careful, balanced, and innovative regulatory responses.

[18] Hill, Rebecca, "CLOUD Act hits Senate to lube up US access to data stored abroad", The Register, February 7, 2018, https://www.theregister.co.uk/2018/02/07/big_tech_biz_back_us_proposals_to_ease_overseas_data_transfers/.

[19] Several countries have already in similar procedures. See Maxwell, Winston and C. Wolf, "A Global Reality: Governmental Access to Data in the Cloud", Hogan Lovell White Paper, 2012, https://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20%2818%20July%2012%29.pdf for a review the legislation of ten high-income countries on this matter.

[20] On MLATs, 24/7 Networks, and other forms of international cooperation specific to cybercrime, see World Bank and United Nations. 2017. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

About the author(s):

Martín Molinuevo, Senior Counsel, World Bank's Macroeconomics, Trade & Investment Global Practice
mmolinuevo@worldbank.org

Simon Gaillard, Consultant, Privacy and Cybersec, PWC
sjhgaillard@gmail.com