Comments of the Computer & Communications Industry Association on Data Protection Regulations and International Data Flows: Impact on Enterprises and Consumers

Bijan Madhani & Jordan Harriman[1]

The Computer & Communications Industry Association (CCIA) submits these comments for consideration by the United Nations Conference on Trade and Development (UNCTAD) for its study on data protection regimes and international data flows. CCIA represents large, medium and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications and Internet products and services. Robust international data flows and interoperable privacy regimes are crucial to the success of CCIA members, as well as other industry sectors that depend on our members' services. CCIA members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[2]

Importance of Cross-Border Data Flows

International data flows have transformed modern trade in goods and services. Data flows create new pathways for commerce and investment, and also allow companies to operate more efficiently. Cross-border e-commerce in goods and services continues to grow in absolute value and as a share of overall trade.[3] Internet platforms allow small- and medium-sized enterprises (SMEs) around the world, especially in developing countries, to reach more customers online with decreasing marginal costs.[4] And as goods production becomes more fragmented and

---

[1] Bijan Madhani is Public Policy & Regulatory Counsel at CCIA. Jordan Harriman is a Policy Fellow.
[2] A list of CCIA members is available at https://www.ccianet.org/members.
[3] The value of cross-border e-commerce could be as high as $350 billion by 2025. In addition, the McKinsey Global Institute estimates that the share of total goods trade attributable to e-commerce grew from 3 percent in 2005 to 12 percent in 2013. See U.S. International Trade Comm'n, *Recent Trends in U.S. Services Trade: 2015 Annual Report*, May 2015, at 116, http://www.usitc.gov/publications/332/pub4526.pdf, and James Manyika, et al. *Global flows in a digital age,* April 2014, at 10, McKinsey Global Institute, *available at* http://www.mckinsey.com/insights/globalization/global_flows_in_a_digital_age.
[4] Some studies indicate that cross-border e-commerce is more prevalent in developing countries than domestic e-commerce. More than half of B2C and C2C transactions in India and Singapore were cross-border in 2013, while the most online purchase by consumers in Colombia, Paraguay, and Venezuela is cross-border. See United Nations Conference on Trade and Development, *Information Economy Report 2015 - Unlocking the Potential of E-commerce for Developing Countries*, Mar. 24, 2015, at 15, http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf.

dispersed into global value chains, data flows have also become essential to non-services fields like manufacturing.[5]

With the growth of digital flows and e-commerce have come concerns about the protection of personal data, and the security of digital transactions and content. These concerns are not just shared by consumers. Protection of data is at the core of the Internet's sustained growth as a platform for expression and trade in goods and services. In fact, the lifeblood of Internet-based industry—which today has grown to include a substantial component of all industries—is the trust that global Internet users have in online platforms.

Though data flows across borders with greater speed and quantity than ever before, laws and regulations on data protection are generally set on a national or regional basis. At times, this can create conflicts of data protection laws due to differing priorities with respect to consumer protection, law enforcement access, and national security exemptions. To ensure that data flows are not unnecessarily impeded, it is essential that countries develop interoperable data privacy regimes that both allow data to move freely, while also providing substantial protections for data belonging to consumers and businesses.

Interoperable regimes are important for a variety reasons. They provide baseline legal certainty that data flows will not be unduly restricted, which gives businesses the confidence to operate and invest freely. This is key for creating an environment for SMEs to participate in cross-border data flows. Such regimes also increase confidence for customers by setting international standards for data privacy and assuring equitable protection for users' data regardless of their country of citizenship.

Interoperable regimes also contribute to the reduction of cost and process burdens on companies conducting international business. Data transfers are not just essential to completing an online transaction; they are critical to the production process for a range of goods and services. And very often, personal data—like subscriber data, employee information, and business contacts—is involved heavily in these production-process transfers.[6] Increased compatibility and flexibility between varying systems can lead to lower barriers to entry for SMEs entering and operating in new or developing markets.

---

[5] See *No Transfer, No Production*, Sweden National Board of Trade, (2015) [hereinafter "Sweden National Board of Trade"], *available at* http://www.kommers.se/Documents/dokumentarkiv/publikationer/2015/Publ-No-Transfer-No-Production.pdf.

[6] *Id* at 13.

Case Study: U.S.-EU Safe Harbor Framework

The long-standing U.S.-EU Safe Harbor framework, in light of its recent invalidation by the Court of Justice of the European Union (CJEU), is instructive as to the high stakes of global e-commerce and the value of maintaining interoperable data protection regimes.

The transatlantic relationship between the United States and European Union is a significant component of both economies, as each is the other's largest market for goods and services.[7] Within that vital relationship, digital trade continues to increase in relative importance as digitally delivered services become more and more essential to overall economic activity. In 2012, the Brookings Institute estimated that U.S. exports of digitally deliverable services to the EU were worth $140.6 billion, or 72% of services exports, and the EU's share of digitally deliverable exports to the U.S. comprised 60% of services exports, amounting to $106.7 billion.[8]

Until its invalidation, the Safe Harbor Framework had been used by more than 4,000 U.S. companies, along with the U.S. subsidiaries of EU companies, to lawfully transfer data about EU citizens from Europe to the United States in compliance with European data protection regulations.[9] In addition to being a direct contributor to the economic benefits that inure from transatlantic digital trade, the Safe Harbor was a boon to transatlantic digital innovation. The efficiency gains from unimpeded cross-border data flows enabled small businesses on both sides of the Atlantic to enter previously inaccessible markets and compete at scale. In fact, a full sixty percent of the companies who had certified compliance with the requirements of the Safe Harbor Framework were small- and medium-sized enterprises.[10]

In October of 2015, the CJEU ruled against the legal underpinnings of the EU-U.S. Safe Harbor Framework. This ruling has had considerable impacts on transatlantic data flows. Thousands of businesses—small and large—that previously transferred personal data from Europe in compliance with the Safe Harbor have had to find alternative mechanisms to ensure that they can continue to do so in compliance with EU law.

The currently available alternatives to permit EU-compliant data transfers are complex legal mechanisms, including binding corporate rules and standard contract clauses.[11] Both options are

---

[7] *See* Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment* 4 (Brookings Institute, Global Economy & Development Working Paper No. 79, 2014), *available at* http://www.brookings.edu/~/media/research/files/papers/2014/10/internet-transatlantic-data-flows-meltzer/internettransatlantic-data-flows-version-2.pdf.

[8] *Id at 12*.

[9] Export.gov, *U.S.-EU Safe Harbor Overview*, http://export.gov/safeharbor/eu/eg_main_018476.asp (last visited Feb. 12, 2016).

[10] Department of Commerce International Trade Administration, *Key Points Concerning the Benefits, Oversight, and Enforcement of Safe Harbor*, *available at* https://business.usa.gov/exportportal?static/Safe%20Harbor%20Key%20Points%2012-2013_Latest_eg_main_068867.pdf.

[11] *See* Press Release, Article 29 Working Party, Statement on Schrems Judgement (Oct. 16, 2015), at

costly, piecemeal, time-consuming, and difficult to implement for even the most sophisticated companies. Expecting small- and medium-sized enterprises to successfully adopt these alternatives, particularly in the short term, to comply with the varying requirements of the data protection authorities of each EU member state would seem unlikely. These other transfer mechanisms are also at risk of being invalidated.[12]

In the long term, the absence of a clear, reliable mechanism for lawful transfer of data across the Atlantic would lead to significant economic consequences. Larger companies could attempt to comply with the implications of the ruling by building costly local facilities for processing and storage of data in the EU. Smaller firms will likely not be able to bear this burden, and could be forced to exit European markets. In 2013 it was estimated that a serious disruption of this very kind to cross-border data flows with the EU would likely cost the EU between 0.8% and 1.3% of its GDP.[13]

Fortunately, a revised agreement between the U.S. and the EU was recently agreed upon. The new EU-U.S. Privacy Shield attempts to strike a delicate balance between the ongoing need for data-driven innovation to benefit consumers and small businesses and to drive economic growth, and a responsible, principles-based framework to ensure consumer protection. The EU-U.S. Privacy Shield is an effort to bridge different legal frameworks for data protection and may be of inspiration for other systems designed to ensure interoperability between other countries and for other types of data.

Costs of Restrictive Data Protection and Localization Regimes

As the invalidation of the Safe Harbor demonstrates, the potential costs to businesses of complying with a number of different data protection regimes can be significant in the aggregate. A recent OECD report highlighted studies which indicate that compliance costs for SMEs not in the ICT sector can increase those companies' IT expenditures by as much as 40%.[14] The report also highlighted another survey, focused on multinational corporations, which found data-related compliance costs averaged over $1 million per year and sometimes could reach $3.8 million.[15] Such costs are high even for large companies. SMEs may not be able to routinely cover these

---

http://ec.europa.eu/justice/data-protection/article-29/press-material/pressrelease/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

[12] *See* Michelle Gyves, *German DPAs Announce Policy Severely Limiting Mechanisms for Lawful Germany-to-U.S. Data Transfers*, Proskauer Privacy L. Blog, Oct. 26, 2015, http://privacylaw.proskauer.com/2015/10/articles/european-union/german-dpas-announce-policy-severely-limitingmechanisms-for-lawful-germany-to-u-s-data-transfers/.

[13] Matthias Bauer, et al., *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, ECIPE (2013), *available at* https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

[14] Susan Stone, et al., *Emerging Policy Issues: Localisation Barriers to Trade*, OECD Trade Policy Papers No. 180, 56 (2015), *available at* http://www.oecd-ilibrary.org/trade/emerging-policy-issues_5js1m6v5qd5j-en.

[15] *Id.*

compliance costs and could exit their respective markets, reducing consumer choices and discouraging innovation.

Some countries have considered or implemented data localization policies, such as mandated server localization or restrictions on where data can be processed. Stated motivations for these policies include the desire to ensure domestic privacy protections, or protect against foreign espionage. However these regulations are often inadequately articulated, vaguely construed, and, therefore, nearly impossible to effectively implement.[16] In fact, rather than ensuring privacy or data security, forced localization creates a host of new valuable targets for hackers. The rise of data localization mandates represents a costly and inefficient alternative to flexible and compatible privacy regimes.

The direct financial resources required to build individual data centers are immense. In 2013, it was reported that the average cost of building data centers in Brazil and Chile were $60.3 million and $43 million, respectively.[17] These sums are considerable even for large companies, and many SMEs would be unable to bear such costs. In addition, the ongoing burden of complying with these mandates would take the place of otherwise productive uses of capital.

It is not just Internet companies that are harmed by localization policies. These policies are likely to hinder broader economic development, rather than promote domestic industry. As a 2011 report notes, 75% of the value of the Internet accrues to traditional, non-Internet centric businesses through productivity gains and easier access to foreign markets.[18] As a result, such policies will invariably harm a wide swath of traditional domestic economic activity and harm a country's global competitiveness.[19] Not surprisingly, economists at the European Centre for International Political Economy (ECIPE) found that current data localization proposals will have significant negative domestic economic effects on the countries that choose to adopt such regimes.[20]

Perhaps more important than the economic costs of data localization and restrictive data protection regimes are their burdens on the Internet as a global platform for free expression. Such regimes can facilitate censorship through blocking access to services and platforms that do not

---

[16] *See* Anupam Chander & Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet*, UC Davis Legal Studies Research Paper No. 378, Apr. 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.
[17] Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill Push for Data Localization*, Wall St. Journal (Nov. 13, 2013), http://online.wsj.com/articles/SB10001424052702304868404579194290325348688.
[18] Matthieu Pélissié du Rausas et al., *Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity*, McKinsey Global Institute (2011), *available at* http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.
[19] One possible example is that local SMEs in countries with forced localization mandates will be less attractive as partners for large companies, since they can't receive personal data. *See* Sweden National Board of Trade at 15.
[20] Matthias Bauer et al., *The Costs of Data Localization: Friendly Fire on Economic Recovery*, ECIPE (2014), *available at* http://www.ecipe.org/media/publication_pdfs/OCC32014__1.pdf.

comply with mandates to store or process data within a particular nation's borders, depriving consumers of a range of content and ideas to which they might otherwise have been exposed.[21]

In addition to their significant adverse economic consequences, overly restrictive data protection and localization regimes can also violate trade obligations if applied indiscriminately or as a trade barrier in disguise. For example, Article XIV of the General Agreement on Trade in Services (GATS) ensures that member countries are not prevented from adopting measures designed to ensure compliance with laws protecting ". . . the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[22] However, this is subject to the requirement that such measures cannot be arbitrary, discriminatory, or a disguised restriction on trade in services.

Developing Flexible Models of Data Protection

A number of countries have developed data protection regimes that permit cross-border data transfers with appropriate protections. No two systems are identical, but each attempts to strike the necessary balance between a responsible, principles-based framework to ensure consumer protection, and the flexibility to interface with regimes in other countries.

For example, Singapore implemented the Personal Data Protection Act (PDPA) in 2012, which permits an organization to transfer personal data overseas if the organization complies with data protection provisions and ensures that the data recipient is bound by enforceable obligations comparable to the PDPA.[23] Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) allows data transfers with the condition that "so long as the transfer is consistent with the use for which the data was originally collected, consent to transfer the data is not required."[24] Meanwhile the U.S., while lacking a comprehensive privacy statute, instead has "a body of laws—a mosaic of federal and state statutes, common law jurisprudence, and public and private enforcement that obligate private entities to protect personal data and respect the rights of data subjects."[25]

---

[21] *See* Hosuk Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law*, ECIPE (2009), *available at* http://ecipe.org/publications/protectionism-online-internet-censorship-and-international-trade-law/.

[22] General Agreement on Trade in Services, WTO, Jan. 1995, https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.

[23] *See* Sidley Austin, *Singapore*, The Privacy, Data Protection and Cybersecurity L. Rev. 212 (2014), *available at* http://www.sidley.com/~/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/singapore/fileattachment/singapore.pdf.

[24] *2015 International Compendium of Data Privacy Laws*, Baker Hostetler 31, *available at* http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf.

[25] Jacques Bourgeois, et al., *Essentially Equivalent,* Sidley Austin 132, *available at* http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf.

Moving beyond domestic regimes, the new EU-U.S. Privacy Shield represents just one prominent example of an effective interoperable framework between nations. Other models exist around the world to promote similar functional compatibility between privacy and data protection laws with cross-border data flows. APEC has developed a voluntary Cross-Border Privacy Rules system (CBPR), which requires participating businesses to develop internal data transfer privacy rules consistent with the APEC Privacy Framework endorsed by APEC economies in 2004.[26] Demonstrating its interoperability with other regimes, APEC has also worked with the EU to streamline the application process for participating companies to use complementary data transfer mechanisms to operate in both regions.[27]

It is important to recognize that interoperability need not require identity of data protection regimes. Indeed, even in the CJEU's decision invalidating the Safe Harbor the Court made clear that "the legal order of a third country need not be identical to be deemed essentially equivalent to the EU data protection regime."[28] Acknowledging that data protection regimes can achieve shared goals through different mechanisms is a key aspect of successful interoperable regimes.

Conclusion

The development of robust interoperable privacy and data protection regimes is vital to empowering consumers and businesses of all sizes to utilize the vast commercial and connective power of digital technologies, while systems that unduly restrict data transfers across borders can have dire economic consequences. National laws and international frameworks should allow for the free flow of data crucial to e-commerce, while ensuring that data protections are strong enough to effectively protect consumers and maintain trust in the Internet as an accessible platform for expression, innovation, and global commerce.

---

[26] The Framework does not impose treaty obligations on member nations. Rather, it sets an advisory minimum standard and represents a consensus across member economies. *See* Sidley Austin, *APEC Overview*, The Privacy, Data Protection and Cybersecurity L. Rev. 19 (2014) *available at* http://www.sidley.com/~/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/apec-overview/fileattachment/apec-overview.pdf.

[27] Angelique Carson, *EU and APEC Officials Agree To Streamline BCR/CBPR Application Process*, IAPP, May 26, 2015, *available at* https://iapp.org/news/a/eu-and-apec-officials-agree-to-streamline-bcrcbpr-application-process/.

[28] *Essentially Equivalent* at 149.