Working Paper
For circulation at the 2017 Global Digital Futures Forum
May 5, 2017

COLUMBIA|SIPA
School of International and Public Affairs

The Fragmentation Mismatch:

Deficiency of Dealing with Fragmentation through Trade Policy

By Hosuk Lee-Makiyama

1. The context to fragmentation

As we are two decades into the digitalisation, data is an established concept in trade policy. Yet fragmentation of the internet is still a matter of great urgency: In pursuit of "re-territorialisation" of digital economic space, 86 data localisation measures are applied in at least 36 jurisdictions (a number that has quadrupling in fifteen years).[1] The eagerness to regulate every new innovative use of data have created regulatory divergences between the economies. Even the trade agreements that are supposed to curb these divergences are fragmented and impose different standards due to irreconcilable policy objectives.

Internet is not the first time in history where a pre-existing model of global governance is caught in a dilemma between maintaining an open economic order, and a sovereigns' right to regulate. But the mismatch between internet and global economic governance is a unique challenge: The rule based system is based on a "bottom-up" approach, that integrates national markets through various instruments of cooperation between them. However, internet was already an open and seamlessly global architecture by the time it became relevant to the trading and financial systems. Hence, bilateral or regional integration (perhaps best exemplified by the Digital Single Market in the European Union) could lead to fragmentation by atomising an open structure that was already global at onset.[2]

This note illustrates how fragmentation occurs across several layers of the economy, serving national objectives on security, political authority and market stability. Such objectives go beyond historical pretexts for economic protectionism. So far, 'hard', strategic objectives have

[1] For a full catalogue of data localisation measures, see ECIPE *Digital Trade Estimates*, accessed at: http://ecipe.org/DTE
[2] Legrain, Lee-Makiyama, *Open Up: How to Fix the Flaws in the EU's Digital Single Market*, OPEN, 2017

trumped the self-punitive damage brought by fragmenting the internet, where data localisation generate net economic losses from 0.7 to 1.7% of GDP, from severe productivity losses.[3]

With few other incentives, digital trade barriers are difficult to address even amongst jurisdictions with similar interests and sensitivities. Negotiations amongst like-minded countries do not necessarily generate positive outcomes. This policy-induced balkanisation is therefore unlikely to be addressed in existing forums for economic cooperation and in the prevailing climate of economic diplomacy.

But fragmentation does not just restrict new services – it is an undoing of the existing framework and revocation of existing liberalisation achieved in trade, investment and taxation, and here lies culmination of the mismatch between internet and governance:

- As 56% of international trade in services relies on access to data,[4] market access in offline services (typically banking, professional services, transports and retailing) can be revoked by simply restrict access to data, despite prior commitments to liberalise such services. This condition has achieved a roll-back of existing GATS and FTA schedules.[5]
- Similarly, notion of 'digital presence' allow tax authorities to withdraw from the territoriality principle on taxation and tax entities that are outside their jurisdiction.[6] As market access via commercial presence (mode 3 in trade parlour) is far more restrictive than cross-border modes of supply, extraterritorial taxation impels towards less cross-border economic exchange;
- On investments, the current provisions against performance requirements in BITs can be easily circumvented through privacy and financial regulations, forcing investors to place their operations in the host country.

2. Taxonomy of fragmentation – extraterritoriality, technical, regulatory and commercial fragmentation

[3] Bauer, Lee-Makiyama, van der Marel, *The Costs of Data Localisation: A Friendly Fire on Economic Recovery*, ECIPE, 2014
[4] Based on assumption used first by *UNCTAD Information Economy Report*, UNCTAD, 2009
[5] Lee-Makiyama
[6] OECD Addressing the Tax Challenges of the Digital Economy, OECD, 2014; see critique thereof, Lee-Makiyama, Verschelde, OECD BEPS: Reconciling global trade, taxation principles and the digital economy, ECIPE, 2014

The conflict between the global nature of internet and the territorial nature of law has led to disputes between different state jurisdictions, producing conflict of forums or inconsistent results. The internet has become subject to a myriad of overlapping jurisdictions and conflicting obligations. Unlike other aspects of international law (e.g. law of the high seas) domestic laws are routinely enforced extraterritorially on online activities. Extraterritorial jurisdiction is often based on the nationality of the legal subject, i.e. a natural person who is a citizen, or a corporation is headquartered in the jurisdiction.

For example, the US tax code is based on worldwide income, that created the current problems of deferment of profit remittances from abroad. Similarly, US Department of Justice has claimed – albeit unsuccessfully – its jurisdiction over e-mail data stored on Microsoft's servers overseas based on the Stored Communications Act (18 U.S.C. §§ 2701) in a criminal investigation.[7]

But the most consequential case of extraterritorial jurisdiction over online space is found in the EU, which typically avoided extraterritoriality.[8] But the General Data Privacy Regulation (GDPR) is applied worldwide for personal information on any European citizen:[9] Applicability of GDPR is not territorially limited, and prohibits international transfers of personal information. Exceptions are limited to jurisdiction that the EU deems to have 'adequate protection', or by using legal instruments (binding corporate rules and model contracts) that impose strict liability for data processors and controllers that transfer the data.

Europe's fragmenting approach is beginning to establish a template for privacy regulation worldwide. In contrast to Europe, China goes extraordinary lengths to avoid extraterritoriality – yet produce similar results. The Great Firewall of China (or Golden Shield, as it is called within China) was initially a technical gateway for monitoring and controlling all internet traffic passing through Chinese borders. The Great Fire Wall balkanised the internet *technologically* rather than through extraterritorial applications of Chinese security laws to the rest of the world. Numerous other examples of *technical fragmentation* exist, such as the long-practiced online censorship in

[7] *Microsoft Corporation v. United States of America*, 829 F.3d 197 (2d Circ. 2016); rehearing request by US Department of Justice *en banc* denied, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017)
[8] Blocking of sales of Nazi memorabilia in *Yahoo v LICRA*, TGI de Paris, 2000; US video streaming of a fashion show where certain logotypes were visible in a manner that violated French copyright laws, but falling under fair use in the US in *SARL Louis Ferarud v Viewfinder*, 489 F 3d 474, New York, 2007
[9] General Data Protection Regulation, Regulation 2016/679

some religiously conservative countries, to the more recent political censorship of Wikipedia and social media in Turkey.[10]

However, China's case differs greatly from Turkey. China had made several relevant commitments in its accession to the WTO for some of the most common online services,[11] and evidently had access to less-trade restrictive censoring techniques (thereby failing the two-tier test of GATS art XIV).[12] As a result, China has gradually moved towards a *regulatory* fragmentation rather than a technical one. China has introduced the Internet Content Provider (ICP) licence, a positive list of services that are deemed safe to use by the Chinese public, while other services may be subject to shut-downs. A licensing regime is more consistent with WTO rules thanks to its weak disciplines on domestic regulation (GATS art VI:4). Foreign investors were also restricted from operating wholly-owned e-commerce or voice over-IP services in China as such services require licenses for value-added telecom services (VAS). Clearly, such regulatory measures have both commercial and public security objectives. China's industrial policies on using indigenous, "secure and controllable" technologies and extremely strict requirements for participation in government procurement support the same dual objectives.

In other countries, the regulatory fragmentation supports objectives have justifications that appear equally uncompromising: A majority (58%) of data localisation measures are due to privacy regulations,[13] based on public perceptions of 'fundamental human rights',[14] an argument that has been proven to be difficult to counter by pointing to their economic costs. Other causes of regulatory fragmentation – such as copyright (disabling content portability across border) or banking regulations (financial supervisors demanding localisation of account data) are by their very nature national instruments confined to their jurisdiction. Such cases of localisation are even exceptions of supranational entities like the EU, addressing geo-blocking only for *pro tempore* cross-border use.

But even in the case where fragmentation does not serve 'hard' national objectives, digital protectionism differs from traditional protectionism, making them more complex to address. The post-war industrial policy engaged in regulatory protectionism to foster national champions,

[10] Turkeyblocks.org, *Facebook*, *Twitter*, *YouTube and WhatsApp shutdown in Turkey* and *Wikipedia blocked in Turkey*, 2017, accessed at: http://Turkeyblocks.org
[11] Online processing services (CPC843)
[12] Hindley, Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law*, ECIPE, 2009
[13] See note 1
[14] See *inter alia* EU GDPR, art 45 for international transfers

but online protectionism does not always follow that logic. To start, traditional protectionism would be pointless for the digital economy that rewards economy of scale in demand (ability to aggregate users), not production (a large factory that enable cheap production and exporting the surplus). For example, Germany's Industrie 4.0 strategy is built on a logic that the country must slow down competition through restrictive intermediary liability to cope with necessary reforms to protect its manufacturing supremacy and domestic media ownership – not necessarily to develop German search engines or social media.

Similarly, some of China's online protectionism is often linked to SOEs as they happened to be a fiscal income source for Chinese provinces, which are prohibited by the central government to raise taxes. Sectors where SOEs were absent (e.g. car-sharing, e-commerce) have been largely left unregulated, or the first sectors be liberalised for foreign ownership. Inability to decentralise China's fiscal structure thereby defers online reforms. Similarly, protectionism of online payments and *fintech* is linked to lack reforms of Chinese capital account and its banking sector that are constantly on the verge of systematic collapse.

Aside from such examples of commercial *objectives* for protectionism, *commercial* fragmentation by abusing pricing and other commercial terms. Absence of fair, reasonable and non-discriminatory (FRAND) terms for interconnection between a foreign and domestic telecom operator bars infrastructural and business services to provide a global service.

Commercial fragmentation by telecom operators often involves telecom SOEs, or wholesale prices that are set a national regulator (as in the *Telmex* case).[15] But non-state commercial entities could achieve same degree of fragmentation, if one local provider is allowed to dominate a market, or if all local telecom operators are colluding. Such allegations have been made against the US telecom and internet markets by foreign entities.[16] Such barriers are horizontal antitrust issues between private players. Similarly, network prioritisation is dominance abuse by an upstream player against a downstream one.

In this context, it should be noted that commercial fragmentation is the only kind of fragmentation that has been reasonably addressed using existing instruments: Antitrust laws

[15] Mexico — Measures Affecting Telecommunications Services, DS204
[16] FCC, WC Docket 16-143 and Docket 05-25, filed by the European Delegation to the United States, accessed at: https://ecfsapi.fcc.gov/file/10419110631001/Ma419.pdf

generally afford national treatment to foreign complainants, and effective WTO remedies against horizontal anticompetitive practices exist in the GATS Telecom Annex, albeit underused.

3. Whither trade governance?

In absence of other effective remedies, extraterritoriality is the new international customary law. This is particularly true for privacy law, an area which is forcefully advocated by the EU. But indirectly, the US is also arguing the case for data localisation and much more fragmenting privacy laws in Russia, Vietnam, China and India. Meanwhile bilateral instruments like adequacy decisions, only enforce existing extraterritorial regimes, rather than become a construct of free internal exchange amongst the signatories, as data is not allowed to flow to a third country. In that regard, they are similar to the limited reach of bilateral tax agreements.

Mutual legal assistance and extradition treaties (MLATs) could have curbed the need for extraterritoriality to address cybercrime, terrorism and privacy violations. However MLATS are today largely discounted. There is a lack of expediency, trust, and a great difficulty in achieving normative harmonisation on privacy and criminal law, making them impractical tools – which was demonstrated between two like-minded countries like Ireland and United States in *Microsoft v. United States*. This is also why harmonisation of privacy laws in international forums like APEC have its natural limits: As regulatory divergences are simply too wide, they contend to best endeavour guidelines based on minimum standards and proportionality. Enforceable rules under the WTO or other multilateral forums seem far off: After all, this is a world where even the 82 signatories of the ITA agreement cannot agree on the most basic non-tariff measures for electrical interference.[17]

As the economic and judicial cooperation fails to address fragmentation, trade disciplines against data localisation and data flows have been singled out as the only way forward – at least to deal with *regulatory* fragmentation. But FTA/RTA negotiations on these matters are effectively about expanding the exceptions, in particular for privacy, security and politically sensitive sectors: A hypothetical renegotiation of GATS art XIV and GATT art XX would most certainly lead to worse results than today.

[17] Electro-magnetic interference and compatibility (EMC/EMI) have been reformed to self-declaration of conformity (SDoC) practice.

Moreover, final TPP texts left generous exceptions for financial services, while the EU is keen to exempt privacy from the two-tier test – or move the burden of proof to the complainant. There are far-reaching consequences of such reversal as securing evidence of bad faith and behind a privacy law, or to prove that its intent is mere disguised protectionism, ought to be impossible. Any data localisation measure currently in place stand a scrutiny against such lax standards.

Given the sensitivities on personal information, one could foresee an argument that such information can be separated from other data *objects*, such as industrial data. The argument is that trade agreements could at least liberalise industrial use of data for the time being. Nonetheless, over 75% of all data online is user-generated,[18] making the majority of data flows personal information by default; the 'industrial use of data' also involves personal data like delivery addresses, information on customers or personnel, as human operators are often logged in while collecting, processing or uploading machine data.

Given the very broad definition of personal data in recently enacted privacy laws, almost any industrial and business data could fall under its scope. All forms of data are also integrated and collated in a data object (say, a file): There are no technical or legal means to separate non-personal information (numbers in a spreadsheet) from non-personal information (author of the spreadsheet embedded in the code). This is the very much the purpose of regulatory fragmentation – to create discretionary powers for an executive to act as gatekeepers to the market by selectively enforcing burdensome rules. Fragmentation has now established "license to operate" regimes, where the executive sets up a positive list of commercial entities that are allowed on the market hinged on nationality or performance requirements.

4. Conclusions

With over 1300 barriers identified affecting the digital economy in a sample of just 65 countries, one could soon argue that we are a *fait accompli,* as there are too many barriers for international treaty negotiations to handle. Economic argument does not seem to sway 'hard' objectives, such as security or fundamental rights. Economic arguments are sometimes even

[18] Austin, Upton, Leading in the Age of Super-Transparency, *MIT Sloan Management Review*, Winter 2016

futile for economic objectives – a draconic online tax law is paid through loss of GDP, in other words corporate revenues and consumer welfare, while governments may actually see their tax base increase. Public choice dilemmas arise as there are different incentives between the public authorities and its subjects.

Third countries find it difficult to incentivise against fragmentation, as balkanisation are consequences of unique structural problems in the underlying economy or the political system. This is the case of the fragmentation caused by both the EU and China.

However, this note is not to provide a justification to fragmentation just because they are uncompromising – but to map why traditional economic diplomacy has so far failed.

In the new political dimension of trade negotiations post-TPP and TTIP, like-mindedness is no longer a recipe for ambitious EPA/FTA outcomes. In fact, similarity is an impediment to successful conclusion of FTAs: Homogeneity (the extent barriers are imposed in same areas) lead to weak outcomes in intra-EU cooperation such as DSM. Regulatory divergences amongst the signatories of TTIP and TISA were narrower than TPP where parties imposed high barriers in completely different regulatory areas.

With no effective cooperation instruments for global openness and rule of law, the global governance system is at a lose-lose situation. As the actors cannot offer credible incentives or threats, and they are left with very few policy options but to block their own economy on reciprocal basis, and thereby contribute to further fragmentation.