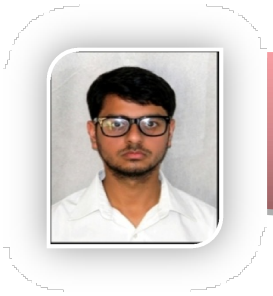
e-ISSN 2582-4570



MANAGING TRANSBORDER DATA FLOWS

Sudhanshu Pathania[*]

Abstract

By its very nature internet is free which allows seamless integration between everyone around the globe. This involves transferring data around at an enormous scale, this exchange of data around makes internet a truly a borderless space. As internet grew, so did the need to regulate various aspects of it. One of such aspect is 'data privacy' and various jurisdictions made rules and regulations regarding it on the basis of how they view 'privacy' as a concept. For instance, EU made laws regarding 'data privacy' around the concept of privacy as a Fundamental Right, on the other hand, the concept of data privacy in USA is very different as their privacy is looked through the lens of dignity and free market. This paper analysis how different jurisdictions try to deal with constant movement of data extra-territoriality while trying to preserve the privacy of their citizens through various approaches which are critically analyzed. This paper also points out how sovereignty of nations is being eroded as laws are not able to cope up with data mobility beyond national borders. The example of 'Schrems v. Data Protection Commissioner' is taken to drive this point home.The final part of the paper seeks a solution of the issue of jurisdiction posed by trans-border data flows by analysing the possibility of a global framework or a solution based on legal pluralism, by weighing them against each other.

I. INTRODUCTION

The world is transformed by internet, everyday internet throws a surprise at us. This is because it has united over 4 billion people on a single platform.[1] People have access to information that wasn't possible before in the history of humanity. It can be best termed as an 'information explosion' with the amount of data that has been generated. One of the best examples that give us some idea about the staggering amount of data that is generated was given in the report by titled 'Data Data Everywhere' in the Economist. Facebook has a library of over 40 billion photos and is every growing adding over 25 petabites of data to their databases that is 167 times the books in America's Library of congress.[2] This colossal amount of data has given rise to its own set of unique problems which are not minuscule by any extent of imagination andtransborder data flows is one of them.

[*] LLM Indian Law Institute. PhD Scholar, NALSAR University of Law.

[1] Internet Usage Statistics, *available at:* https://www.internetworldstats.com/stats.htm (last Modified: March 25, 2021).

[2] Data, Data Everywhere, *available at:* https://www.economist.com/special-report/2010/02/25/data-data-everywhere (lastVisited on April 3, 2021).

Personal data is the oil of 21st century, one who controls data controls economy, this becomes apparent when we see that Alphabet, Facebook, Amazon and Microsoft raked in 25 billion dollars of profit amongst themselves in 2017 alone.[3] Personal Data is the crucial raw material on which economy would run in the future. This data when processed becomes valuable to the companies who use it as per their business models but also pose serious threat to an individual's privacy. Moreover, when we take into account the fluid nature of Internet where this data crosses borders seamlessly, protecting privacy of individuals become even more cumbersome.

During the infancy of internet, there was very little transborder data flows, and whatever there was it was all point to point exchanges however, today transborder data flows have grown manifolds. There is hardly any empirical data available that shows to what extent such transborder data flows have increased however it doesn't require a genius to make an intelligent guess that the transborder data exchanges that were happening in the in 1970 is a mere fraction to what is happening today. Because, Internet shows literally no regard for the International border thereby most of the data routed today does not give regard to the sanctity to international borders we can assume that a big chunk of it would fall under transborder data flows. In 2016 Cisco published a white paper which said that global IP reach had reached 1 zettabyte.[4] To give an idea of scale, 1 extabyteis the size of 36000 year long HD video and 1 zettabyte would contain 1000 such videos.[5]

I have used 'fluid' and 'something that shows no regard for the international borders' for internet and it is because internet is structured on technological lines and not on geographical lines, in other words there is a good chance that if I send over a file win the same city, it is not an impossibility that it has been routed through a server not in that country but another country by the ISP.[6] Due to this technological complexity, the lines between transborder data

[3] The World's most Valuable resource is no longer oil, but data, *available at:* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited on April 3,2021).
[4]VNI Global Fixed and Mobile Internet Traffic Forecasts *available at*: https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html(last visited on April 3, 2021).
[5] What is Zettabyte? By 2015 the Internet would know says Cisco *available at*: https://www.theguardian.com/technology/blog/2011/jun/29/zettabyte-data-internet-cisco (last visited on April 3, 2021).
[6] European Data Protection Supervisor, 'Cloud Computing in Europe' *available at*: https://edps.europa.eu/data-protection/our-work/publications/opinions/cloud-computing-europe_en (last visited on April 3, 2021).

transfer and data transfer within the country has blurred so much that for regulatory purposes it would be safe to assume that all data transfers are transborder data transfers.

II. TRANSBORDER DATA FLOWS: GOOD, BAD AND THE UGLY

To apply regulations on transborder data flows, we need to first define what transborder data flows are. The vice with defining transborder data flows is that each definition comes with its own set of flaws and more one tries to resolve them through each amendment, you find yourself staring at a host of new flaws. From EU directive[7] to Asia Pacific Economic Cooperation privacy framework[8] and even GDPR[9] have tried to define transborder data flows. And then there are a few like the Canadian Personal Information Protection and Electronic Documents Act (hereinafter referred as PIPDA) which does not distinguish between 'transborder data transfer' and 'data transfer' where both are considered the same.[10]

One of the reasons defining it has become such a cumbersome task is that data can cross borders not by actively being sent across borders but by being sent across individuals and not to forget transfer of data as a part of the internet structure as discussed previously(although that can excluded from the working of any regulatory mechanism through safe keeping provisions).[11] It is important to differentiate that such data transfers might happen both as a deliberate action but as a part of the process as well. Most authors are of the view that such 'mere transactions' should be kept beyond regulations however post NSA I am sceptical that even such data transfers are kept beyond surveillance states like USA and China.[12]

Along with the risks, transborder data transfers come with a bunch of benefits where the benefits seem to outweigh the risks especially when the risks are properly managed. I have

[7] EU Data Protection Directive, 1995, art 25(1).
[8] APEC Privacy framework has no clear definition of transborder data flows but instead uses various terminologies like 'cross-border information flow' and 'cross-border data transfer' interchangeably.
[9] General Data Protection Regulation, 2016. Ch. V.
[10] Guidelines for Processing personal data across borders *available at*: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/ (last visited on April 3, 2021). In the explanation to the act, transfer is explained as 'use' by the organisation. By defining the transfer in terms of how and when data is used by an organisation the Canadian PIPED Act have very smartly avoided the question and ambiguity of when does data crosses the borders and when the act would be applicable.
[11] *Supra* note 6.
[12] Government Surveillance: Last Week Tonight with John Oliver *available at*: https://www.youtube.com/watch?v=XEVlyP4_11M (last visited on April 3, 2021).

categorised it under three heads, benefits under 'good', risks under bad and the evil aspects under 'ugly'.

Good: From whole society to individuals, transborder data transfers are of immense benefit. In society, the one such example is that of Arab Spring where democratic ideas like freedom of expression and equality which originally were known only to small and affluent strata of the society, were enforced through a revolution and multiple monarchs were dethroned. These 'western ideas' found place within the streets of Libya and Tunisia because of this open-ness of Internet.[13] On an individual scale the effects are not that profound but still important where individuals get access to a host of services which otherwise would have remained only to a few. Another example is that of Khan Academy, this YouTube channel by an Indian-American who teaches mathematics and other science related subjects from 8th standard to College level. Thanks to internet everyone around the world benefits from his videos.[14]

Corporate is another beneficiary of transborder data transfer because they get access to new markets which otherwise would not have been possible.

Bad: There are certain downfalls of transborder data transfers, which can be seen at the levels of Government and Corporations. It makes difficult for the government to track online frauds and tracking internet based crimes have become more difficult for the governments around the world. Corporations have also found it difficult to protect their intellectual property on the internet. A 2007 study found that IP theft cost companies billons of dollars. According to TV privacy forecast report, the loss due to online privacy would double to 51.5 billion by 2022.[15]

Ugly: If 'good' paints a rosy picture then 'ugly' paints a bleak one where an individual has no privacy and Orwellian Dystopia has come true.[16]Transfer of personal data to states without

[13]How the Arab spring engulfed the Middle East – and changed the world *available at*: https://www.theguardian.com/world/ng-interactive/2021/jan/25/how-the-arab-spring-unfolded-a-visualisation (last visited on April 3, 2021)
[14] Khan Academy, Results span Countries and Grade Levels, *available at*: https://www.khanacademy.org/about/impact (last visited on April 3, 2021).
[15] Quantifying loss due to streaming privacy, *available at*: https://cleeng.com/blog/streaming-piracy-quantify-revenue-loss#gs.44acin (last visited on April 3, 2021).
[16] Why Orewll's 1984 could be about now, *available at*: http://www.bbc.com/culture/story/20180507-why-orwells-1984-could-be-about-now (last visited on April 3, 2021).

adequate data privacy regulation jeopardizes privacy and makes individual's data susceptible to unauthorized use. There is a consistent threat of surveillance by foreign governments which further hinders free flow of data across borders as the technological companies would prefer. I must add that this is not any unfounded suspicion as post NSA revelations any email that has been routed through a server within USA could be accessed by NSA does not sound very improbable.

III. TRANSBORDER DATA: REGULATIONS

Main reason various states have enacted regulations is because in today data protection is very closely related to an individual's privacy.[17] Another reason why states enact laws to regulate transborder data flows is to preserve its 'Informational sovereignty'.[18] Informational Sovereignty at best can be understood as the ability of a country to control what happens to the data of its citizens beyond its borders. If a country lacks such ability where it is unable to control data, then its decision making capacity is said to be compromised. Many governments have expressed concerns that transborder data flows if left unregulated would impede their National Economic Sovereignty.[19]

However, while regulating transborder data flows, states try not to break the internet by hindering the free flow of data. Thereby regulations are to be made in such a manner that Internet stays fluid.

Although there is a consensus that regulating transborder data transfers is a necessary, how it is done is a totally a different manner. Different regimes have found different ways to look at regulate transborder data flows, for instance EU calls regards Data Privacy as a person's Fundamental Right.[20] Even in *Rotaruv*. *Romania*, the European court of Human Rights interpreted Art 8 of European Convention of Human Rights where a person's right to private and family life was given a wide interpretation to include data privacy as well.[21] By considering data privacyasa person's basic Fundamental Right, Transborder data transfer regulations in EU are made exceptionally strong.

[17] Cyrus Farvivar, *Habeas Data: Privacy* v. *Rise of Surveliace Tech* 35 (Melville House, UK, 2018).
[18] United Nations, "Report of Commission on Transnational Corporations of the UN Economic and Social Council", (July, 1981).
[19] John M.Edger, "Emerging Restrictions on Transborder Data Flows: Privicy, Protection or Non Tarriff Trade Barriers" 10 *Law &Pol'y Int'l Bus* 1055 (1978).
[20] *Supra* note 9, art 1.
[21] (2000) ECHR 191.

On the other hand there are many regimes like USA, where data isn't looked from the same lens as that of EU and has taken a different approach. Here, a clear influence of the capitalist economy is visible where ease of doing business is takes centre stage. In US privacy means right to be let alone and have evolved so as a protection against intrusion in one's personal space. In USA privacy is viewed from a prism of *liberty* and *free market*. These values trickle down to transborder data regulation where it looks like'less regulation is more convenience' approach is used by the US government. Such a regulationwould promote free flow of data and zealous nature of the American government to promote their business interest over privacy concerns is clear.[22]

The above two examples explain how culture is an important factor in deciding how privacy norms are followed in different jurisdictions. This also explains why there is no straight jacket formula in dealing with the issues of data privacy and transborder data as every place has its own cultural norms according to which it chooses how to implement regulations to protect data privacy.

One major aspect about transborder data regulations is how they deal with the privacy issues once data is transferred to a third countries and what laws would apply then. Two major approaches to this are geographical based approach and organisation based approach. It is also known as adequacy versus accountability approach.

Geography Based Approach is also called as *Adequacy* approach is an approach to regulate data transferred to a third country based on the legal system of that country and the protection to data that it provides. It is called the adequacy approach because this approach requires that a minimum standard of protection as per the data exporting country should be provided and only if a minimum standard of protection is provided the exporting country would allow transfer of data to a third country. There are a number of regional and national legislations which follow this approach, some of the major ones are:

[22]Tarrence Craig and Marry E Ludolf, *Privacy and Big Data* 13 (O'rille, Sabastapol, 2011).

i. EU Data Protection Directive – Art 25 of the directive asks for adequate level of protection to allow transfer of data to a third country.[23]
ii. EU's General Data Protection Regulation – This regulation replaced the Data Protection Directive in March of 2018 and follows the same adequacy principles that the directive followed. Chapter 5 of the regulation talks about 'Transfer of personal data to third countries'. GDPR adequacy requirements are more stringent than that of the directive where Art 45 states what adequacy is and what steps are required by the commission so as to ensure adequacy.[24]
iii. Council for European Protection 108 - Equivalent Protection requirement is made within the convention. While the adequate protection asks for a 'minimum protection to data', equivalent protection is different at it requires same levels of protection that is provided by the convention.[25]
iv. Andorra – A level of protection for personal data equivalent to that established by the law[26]
v. Bosnia – The Same principles of data protection as provided by law on protection of personal data.[27]

These were a few countries and regional organisations which follow the Adequacy approach with each having its own set of principles to define what adequacy is.

The supporters of this approach state that by using this approach they are encouraging countries to enact data privacy laws so that they could attract data exports from those countries and therefore are promoting the principles of privacy to countries which have not adopted them already.

I have a twofold criticism of this approach *firstly,* where a country has to decide whether another country's laws are adequate or note, such a decision is based more on political considerations than legal ones. Irish government's refusal to grant Israel the adequacy

[23] *Supra* note 7.
[24] *Supra* note 9, art. 45.
[25] Council for European Protection - 108, 1981, art.2(1).
[26] Qualified law on Personal Data Protection, 2003, art. 35
[27] Law on Protection of Personal Data, 2006, art. 8.

certificate because Israel was involved in forgoing passports of Irish nationals is an apt example of how politics influences such decisions.[28]

And *secondly,* this approach interferes with the sovereignty of a third nation by arm twisting it into enacting a legislation similar to yours which might not be right for it based on its socio-economic conditions.

Organisationally based approach or otherwise known asthe *accountability* approach. While the geographical approach puts onus on the third country to make sure that their laws are adequately equipped so as to protect personal data. On the other hand in accountability approach, onus falls on the organization or the company which exports data to a third country. As per this approach, adequate measures are to be taken by the data exporters so as to make them accountable for processing personal data in third countries. Malcom Crompton explains this approach in the following words 'This approach ensures that the original collector of personal information remains accountable for compliance with the original privacy framework that applied when and where the data was collected, regardless of the other organisations or countries to which data travels subsequently'[29]

Accountability approach just like adequacy approach asks for the parent legislation to be implemented, however in this approach implementation is directly on the company who had initially collected personal data instead of channelling it through another sovereign country by arm twisting their legislature to adopt the parent country's Data Privacy measures. Organisations implement these measure through 'due diligence' measures through contractual obligations on other organisations operating in the third countries to abide by the parent country's data privacy rules.

The major advantage that this approach has over adequacy approach is that it is easier for the parent company to implement their laws on a private company by themselves upon violation of someone's Data Privacy rather than asking a sovereign country to do so on their behalf. There is a major disadvantage to this as well, when there is a violation of data privacyprincipals in a third country it becomes difficult for the data controller of that country

[28]Ireland to block EU-Israel data hoover, *available at*: https://www.theregister.co.uk/2010/07/12/ireland_israel_passport/ (last visited on April 3, 2021).
[29] Malcom Crompton, "The Australian Dodo case: An Insight for Data protection regulation",*Boomberg Privacy and Security Law Report* 181 (2009).

to ascertain who is the parent company that had authorised such transfer outside to a third country.

IV. EXTRATERRITORIAL APPLICATION OF FUNDAMENTAL RIGHTS LAW

One of the issues that come with the transborder law is the problem of jurisdiction. EU has taken an expansionist approach to this problem. By defining data privacy as a Fundamental Right, they have laid groundwork for applying earlier Data Protection Directive and now GDPR beyond its jurisdiction. Although Europe Convention 108[30] defines jurisdiction based on territory only, yet there have been constant proposals to expand as their data privacy laws are Fundamental Rights so they should be given the same coverage as European convention of Human Rights. Many instances have come up where the European Court of Human Rights has caved into such demands by slowly expanding the jurisdiction of EU's data privacy laws beyond its borders. In one of the most prominent cases, the European Court of Human Right has extended the jurisdiction under European Convention of Human Rights outside the territories of European Union. However, the extent of it was kept limited to the instances where regulatory state had control over terror where the said violation had happened.[31] European data privacy laws, being Fundamental Rights and hence an extension of European Human Rights Law theoretically can be applied in transborder data violations as well. However, there are jurisdictional issues like the knowledge of actual place where the violation of Human Rights have been committed which is difficult to ascertain in case of transborder data violations.

In SWIFT case,[32] the Belgian Privacy commission considered the question that to what extent it could enforce compliance extraterritorially in deciding whether that could enforce Belgian Data Privacy laws in US or not. In the final order the commission finally caved in and said 'Belgian law does not apply to US and any qualification would remain purely theoretical and without effect.' SWIFT was a co-operative company which provided reliable messaging services to a number of financial institutions. It was established in Belgium and for providing reliable service it maintained databases in Belgium and in USA which were mirrors of each

[30] *Supra* note 24.
[31] *Al-Jaddav. United Kingdome*, (2011) ECHR 1092.
[32] Belgian Privacy Commission publishes decision on 'SWIFT case' *available at:*https://www.lexology.com/library/detail.aspx?g=853bdcbb-32e6-4e72-88c0-89376ec6c60b (last visited on April 4, 2021).

other. Post 9/11 USA sent subpoena to access the mirrored database which came under US jurisdiction. When SWIFT gave access to authorities the whole question of violation of EU's Data Protection Directive came into the picture and the Belgian Privacy Commissioner had to decide whether it could enforce compliance of Belgian privacy laws in USA.

One of the most important judgements in the field of transborder data flows came in the case of *Maximilian Schrems*v. *Data Protection Commissioner.*[33]In this judgement, the court invalidated the US-EU safe harbour agreement which the council had said provided adequate protection to data transfer from EU to US. This case became more significant because it came post NSA snooping revelations. The petitioner in this case had specifically filed a case after Edward Snowden had revealed details about snooping done by NSA on a massive scale on number of people around the world including US and EU citizens.[34]

On October 16th 2015, CJEU gave a judgement. While dealing with adequacy principal, judgement said that the third party needs to provide guarantee which is equivalent to that provided under EU law. In the same paragraph, the court gave the justification of the 'Equal' requirement by saying that Data privacy is a fundamental Right and thus equal requirement is reasonable.[35] This is a flawed interpretation of the EU laws, both of the directive and that of GDPR as they required only adequate protection and not equal protection.(Although when the judgement case directive was under force and GDPR replaced it later on, still even GDPR with its stern requirement does not ask for equal protection).

There are many aspects that are both intriguing and questionable of this judgement, I would stick to those parts which specifically deal with application of data protection rights to third party countries. In this relation what they said in paragraph 44 is interesting:[36]

> EU law did apply to data transfers under the Safe Harbour becausethe operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive 95/46.

[33] ECJ Case – C 362/14.
[34] Christopher Kurnes, "Reality and Illusion in EU Data Transfer Regulation Post Schrems", 18 *German Law Journal* 881(2017)
[35]*Supra* note 32, paragraph 73.
[36]*Supra* note 32, paragraph 44.

This for all practical purposes imposes the EU law on all third countries as the manner in which Internet works, data has to be routed through a third country. This is exactly what Anu Bradford calls the Brussells effect in which EU itself engages in unilateral regulation of the global markets and sovereignty of these countries takes a hit.[37]Adding to this new understanding of adequacy principle and EU law applying to literally everywhere data flows, DPAs are given more power under GDPR as much as stopping data flows to a third country which has the potential to break the internet and not in a way celebrity selfies do.

This is a beautiful illusion, at least to European eyes, because it envisions a world where the reach of EU data protection law extends globally; where attempts by foreign intelligence agencies to access the data of Europeans are repelled through the use of procedural mechanisms; and where DPAs police the Internet and quash attempts to misuse European data. Yes, it is nothing but illusion as everything said has little to do how internet works on ground.

V. A GLOBAL FRAMEWORK

The above stated problem is because of the fact that there is a lack of global framework where every jurisdiction is trying to achieve its own ends through ways that suit them the best. There seem to be two set of groups, one who favours free flow of data with little or no regulation and the other which is trying to look at the data privacy implications of transborder data flows. Due to this, there are considerable differences in regulations in different states and these differences as explained earlier are partly due to the cultural differences and partly because of different economic and political requirements from personal data.

Current Transborder data flow regulations as a form of legal pluralism

Current transborder data flow regulation can be best understood as a form of legal pluralism. The manner in which these regulations have come up over tie they can be best defined as legal pluralism. In absence of any true hierarchical structure and authoritative government a pluralistic approach seems appropriative. Following are some characteristics which point towards a pluralistic structure –

i. Conflicting regimes in public International Law with a clear lack of hierarchy.
ii. Differing hierarchies in Human Rights

[37]Anu Bradford, "The Brussels effect", 107 *NorthwesternUniversity Law Review* 1(2013). Whole Article 13 of the EU copyright amendment laws is another example of Brussels effect.

iii. Conflict of laws on the internet, where there is a differing and sometimes conflicting concepts of Fundamental rights.

In a pluralistic system, there is an absence of *Grundnorm*that would allow resolution of conflicts which is precisely the situation in which we find ourselves with regards transborder data flows.

Binding International Agreement as a Solution?

Most of the time the answer that comes up with regards to problems like these is a single binding international agreement which would give minimum requirement for data privacy as a basic requisite that has to be followed by everyone. It seems a simple answer to a very complex answer and while in theory it might work, but in practice it would be very difficult with such diverse requirements of each nation state with regards to data. While some countries prefer free flow of data so that their companies could mine it, there are others where data privacy is a fundamental right. More you dive deeper into the problem more you start to think that there cannot be a middle ground between the two, put cultural differences within this mix and it becomes chaos. In EU, data localization is seen as a way to protect people's personal data while in India when Sri Krishna committee report became public, privacy experts were up against arms against the government's plans to localize data as it might lead to surveillance on the citizens by the Indian government.[38]

Then there is the issue of which global institution would be able to draft such a treaty. Some international bodies like UNICITRAL and UNIDROIT do come to mind that have the expertise in the field of internet and privacy respectively but don't have the diplomatic strength to see through such a politically charged treaty.

It seems that we are falling prey to the street light effect where we have a tendency to look for answers in places where they are easiest to look at.[39]In my view pluralistic approach is the right way forward where the regulations grow with time rather than a powerful International agreement on the lines of TRIPS which in all practicality is impossible to make due to conflicting interests of all the parties involved. If we accept that the framework is fragmented

[38]Srikrishna Committee: The Good And The Not-So-Good In The Data Protection Committee's Report *available at*: https://www.bloombergquint.com/law-and-policy/srikrishna-committee-the-good-and-the-not-so-good-in-the-data-protection-committees-report (last visited on April 3, 2021).

[39] The streetlight effect is a concept that comes from an old joke where a drunk is trying to look for his keys under a streetlight not because he lost them there but because where he lost them it is dark over there.

and they try to harmonise over time it rather than to force through an International treaty we would achieve better results. This method would allow the countries to mature overtime which allows harmonisation of norms and eventually in a natural and phased manner consensus would be formed between two opposing ends of the spectrum.

This being said there are certain reforms in the current pluralistic structure that can be made to make it more robust so that flow of data is not hindered and privacy concerns of parties like EU are also addressed.

i. *Agreement with regards to data which requires extra protection*: Internet consists of all kind of data with variable importance, a person's weight is not of that sensitivity rather than his financial data. Hence, agreement between various states can be reached with regards to what can fall under 'sensitive data' and what cannot. And what level of extra protection should be provided.
ii. *Technological Measures*: Technological measures are required to be put in place to promote privacy of data transferred internationally like double encryption. On the other hand regulations need to be sensitive of technological realties, how data is transferred would always depend on the technology in place and not on what regulation is present in that jurisdiction.
iii. *Greater cooperation*:Cooperation between various nations is required to bridge the gap between them and make transborder data regulation more robust. The 'endgame' of pluralistic regime is to enable transborder data flows in a more secure manner where privacy isn't compromised upon and that can only be achieved when countries become more cooperative.

In concluding remarks, I would say that transborder data is like globalization, we can't do away with it. It is better to make peace with it and let it evolve for the benefit of everyone. There is always a natural desire to find a single straight jacket solution to our problems, but Internet is fluid and for a fluid and ever-changing problem a single top-level solution won't suffice.

V. CONCLUSION

The dependence of this data driven world is going to increase on algorithmic decision making which will make the movement of data across borders even more voluminous and as the internet is structured presently, there will be more confrontations between various data

protection regimes. It is pertinent that a minimum standard of privacy is agreed so that the interests of the states protecting privacy of their citizens and the interests of the corporations mining data are given due regards and flashpoints like the one with Ireland are avoided in the future.