Bridging the Gap Between Right to Trade and Right to Privacy: An Application of the 'Principle of Inter-Operational Equity'

Ahmed Adib*

Abstract: Trade and privacy both have persisted concurrently since time immemorial without any contradiction. Recently, they are conflicting with each other on various grounds in particular cases. The right to trade and the right to privacy are indivisible and utmost importance should be given in keeping the enforcement of these rights uninterrupted. Respective and regulatory authorities have failed to shield the citizens' right to privacy due to loopholes and lacunas in the remaining laws. In these circumstances, by analyzing the present scenario, existing laws, conventional dispute settlement mechanism, and finally, introducing the 'principle of inter-operational equity' backed by morality and good conscience, this qualitative research aspires to pave the way in bridging the gap between the right to trade and right to privacy in this digital era. Although the research emphasizes on the disputes of the United States (hereinafter as "the US") and the European Union (hereinafter as "the EU"), it is hoped that national and contemporary international issues regarding trade and privacy outside the jurisdiction of the EU and the US can also be settled by the principle introduced herein.

Keywords: Trade, privacy, equity, data protection, and inter-operational equity.

1. Introduction and Rudimentary Notion

"Equity is the correction of law which is defective on account of its generality." ---Plato

The term 'equity' has been derived from the Roman word 'acquitas' which denotes levelling or equalization. Etymologically, equity refers to levelling down any denial of justice or arbitrary preferences.[1] 'Equity' may, however, also be used in a dissimilar and more limited sense. An equitable judgment or decision may be one that is neither intended to inaugurate a new arrangement of precedents nor based on a prevailing rule of law.[2] Its only aim is to do justice between the parties in a (particular) case categorized by the creation of facts unlikely to be repeated practically in the identical or similar way.[3]

Nevertheless, in the present world, wide-ranging dossiers exist containing information about each one of us. Government and private companies have stored

* The author is an Advocate at the Dhaka Judge Court, Bangladesh.

1 Aqil Ahmad, *Equity, Trust, Fiduciary Relations & Specific Relief* (14 edn, Central Law Agency 2008) 2.

2 ibid, 1.

3 ibid.

these dossiers in computer databases.[4] The complications caused by these advancements are profound. As John Dewey rightly observed, "a problem well put is half-solved", we cannot certainly fix a problem until and unless we know the damage that it is causing.[5] Today, the right to privacy is not a tenet only to be discussed in constitutional seminars or workshops, nor it is merely the subject matter upon which judgment is rendered by the superior courts. It has profound financial impact as well including economic security, consideration in the annual budget on improving national cybersecurity, mechanism to secure central reserve, and so on.

Another aspect is – if one party is enjoying the right to trade, another party's right to privacy is being violated. This dichotomy is taking place sometimes intentionally and sometimes without *malafide* intention. However, whatever the intention is – its negative impacts are fatal. Such effects starting from a family, going through national anarchy and international cold war, have the potentials to draw an end even through a world war. For better understanding, the right to trade can be thought identical to the right to information as in both the cases, the philosophies are not that much different, whereas, right to privacy can be considered similar to trade secret.

The creation and existence of law can hardly be thought of without bearing in mind the swift impact of morality. Philosophies of criminology and penology are not worth discussing in this paper because they may distort the present study and may, to some extent, lead us to uncertainty, ambiguity, and vagueness. There is still a debate continuing regarding which one can pave the way to keep anybody away from committing a crime or felony – it may be brutal but effective laws or can it be 'morality'. Nonetheless, the pivotal thing is 'morality', saying more specifically 'good conscience', should prevail not only over personal interests but also the interests of the community, and finally, over the citizen of the universe at large.

Accordingly, all the persons, regardless of being natural or legal (also known as an artificial, juristic or fictitious person), conducting any legitimate trade which may be of providing information or data or so on, should not engage in any activity which has the potentials to violate anyone's constitutional or human rights, especially, the right to privacy. Hence, in all aspects of conducting a trade or enjoying the right to information or while dealing with trade secrets, all personnel should apply the equitable philosophy of 'equity, justice, and good conscience', and applying such philosophy, while conducting trade and protecting privacy, may be termed as 'principle of inter-operational equity'. The principle denotes that

[4] Daniel J Solove, 'The Digital Person: Technology and Privacy in the Information Age' (2004) 42(9) GWU Law School Public Law Research Paper 13 <https://ssrn.com/abstract=2899131> accessed on 1 November 2020.

[5] ibid, 6.

in all aspects (which include but are not limited to the operation of trade, conducting business works, promoting freedom of expression or right to information, or protecting the right to privacy), the mentioned equitable philosophy of 'equity, justice, and good conscience' should be applied.

The principle also refers to that all the bodies or persons should adopt the equitable philosophy while conducting their respective duties. Saying more specifically, the judge while pronouncing or rendering judgment should apply the 'principle of inter-operational equity', the owners/employers of tech companies should inflict the philosophy of equity while conducting business, the employee of any tech company is also expected to adopt the philosophy of equity while dealing with clients or the information of clients. The principle also denotes that the judges ought not to follow (or adopt) the literal rule of interpretation when such adoption may cause either undue hardship or unfair advantage to any of the parties. The respective authority should not adopt the very words of law when such adoption leads to parties towards vagueness and ambiguity. The decision should be based on morality, equity and good conscience. Therefore, in all sorts of operations or functions, applying the philosophy of equity, justice and good conscience (in order to bridge the gap between trade and privacy) is referred to as the 'principle of inter-operational equity'.

2. Scenario of Privacy Protection within the European Union

It can undoubtedly be said that trade in services is significantly assisted by universal flows of data and information technologies.[6] Recently, statistics show that cross-border data flows are now putting forth more impact on global GDP than the trade in goods is implying.[7] Permitting global data flows, which includes individuals' private data, has acquired centre phase in international strategy efforts, which are powerfully backed by stakeholders than the industries.[8]

The EU's latest General Data Protection Regulation (hereinafter as "GDPR") comes into effect on 25 May 2018 which has a wider ambit and stronger enforcement

[6] Kristina Irion, Svetlana Yakovleva and Marija Bartl, 'Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements' [2016] independent study commissioned by BEUC et al. Amsterdam, Institute for Information Law (IViR), 1.

[7] McKinsey Global Institute, 'Digital Globalization: The New Era of Global Flows' [2016] McKinsey & Company, 83 <http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20Te%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx> accessed on 9 July 2020.

[8] E.g. UNCTAD, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' <https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> accessed on 9 July 2020.

strategy than the 'Data Protection Directive'[9] which is replaced by the GDPR.[10] The recent news focusing on transatlantic data flows or on data leaks connected to Facebook[11] has covered the influence of GDPR on developing countries because numerous developing countries export "digitally delivered data-processing and business services, which require international flows of data".[12] In 2015, these services, including fiscal accounts, tax returns, health transcriptions, and diagnostics, etc., added more than $50 billion worth to the exports from developing countries to the EU.[13]

Moreover, international trade agreements tend to hold 'no direct effect' on the very ground that the agreements are not self-executing and not straightforwardly conferring rights on natural or legal persons.[14] Research on "post-2008 free trade agreements conducted by the EU" demonstrates that it has already become an extraordinary characteristic to incorporate a so-called 'no direct effect' provision/clause in the agreement.[15] Such 'no direct effect' clauses generally appear in the guise of four different modes: (a) as a general/wide-ranging clause in the agreement, excluding direct consequence of the agreements; (b) as a clause that the decision under the dispute settlement scheme does not generate obligations and rights for the natural or artificial person; (c) "as a clause in the schedules of commitments"; and (d) as a clause/provision in the granting or approving council decision.[16]

In the ***Hannover case***[17], the European Court of Human Rights (hereinafter as "ECtHR") states that the key factor in protecting the private life against the freedom of expression ought to lie in the involvement that the (published) photos and articles are made for the sake of general interest. In this case, Princess Caroline

---

[9] The EU espoused the Data Protection Directive (DPD) in 1995 which was the first wide-ranging data safety structure aiming at protecting the privacy rights for the processing of private data. See, Irion, Yakovleva and Bartl (n 6) 3.

[10] Aaditya Mattoo and Joshua P Meltzer, 'Resolving the Conflict between Privacy and Digital Trade' (*VoxEU.org*, 23 May 2018) <https://voxeu.org/article/resolving-conflict-between-privacy-and-digital-trade> accessed on 27 November 2020.

[11] Cambridge Analytica, a political information firm employed by President Trump's 2016 election campaign, accessed data on 50 million Facebook users as an approach to recognize the characters of American voters and to influence their conduct. See, Kevin Granville, 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens' *The New York Times* (19 March 2018) <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html> accessed on 10 July 2020.

[12] Mattoo and Meltzer (n 10).

[13] Matthias Bauer and others, 'The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce' [2013] European Centre for International Political Economy (ECIPE).

[14] Irion, Yakovleva and Bartl (n 6) 16.

[15] Aliki Semertzi, 'The Preclusion of Direct Effect in the Recently Concluded EU Free Trade Agreements' (2014) 51(4) Common Market Law Review 1127.

[16] ibid, 1129.

[17] (2005) 40 EHRR 2.

of Monaco asked to prevent the dissemination of photographs of her and her children engaging in daily activities such as shopping, horse riding, dining at a restaurant and so forth.

In ***Von Hannover v Germany***[18] (No. 2), two distinct magazines had issued a series of photographs of the applicants regarding their private affairs while on holiday. The German Court declined to grant (or render order of) injunction since such publication was justified on the ground of legitimacy encompassing a public interest story about the ailing health of (her) father - Prince Rainier III, the reigning monarch of Monaco. The ECtHR eventually ended up with a few observations that the following criteria are pertinent with a view to striking a balance between the right to freedom of expression and the right to (respect for) private life: (a) the debate of general interest should be considered and subjective approach, in this regard, should be followed as it varies from person to person, place to place, circumstances to circumstances; (b) the familiarity of the person concerned must be taken into consideration, i.e., whether s/he is a well-known person or not. Along with the mentioned considerations, the subject of the report is also significant; (c) whether the news/information about the person concerned is already disclosed or not, i.e., the earlier activities (including both acts and omissions) of the person regarding the dissemination of the information; (d) whether the newspaper is a local or national one, i.e., content, consequences and form of the information; (e) circumstances under which the photos were captured. In this case, it was held that there was no brech of law.

However, it is noteworthy that subject to a few notable exceptions like the above mentioned (***Hannover*** *No. 2*) case, the EU, being one of the cornerstones for showcasing substantial trial and judgment worthy of being cited widely almost all around the world, has not been applying the philosophy of equity, justice and good conscience in the proposed (and at an expected) manner which is required to protect any of the parties to the dispute from unusual hardships or to prevent any party to get an unfair advantage over another party. It should be borne in mind that the more natural application there is while applying enactments and rendering judgments that have the potentials to ensure justice amongst the parties, the more substantive the remedy will be.

3. Privacy Protection in the US

Previously, communities were intimate and small, and individuals' information was conserved in the memory of family, friends, and neighbours, and such information was shared and circulated by storytelling and gossip.[19] Today, the principal mode of expanding "information is not through the flutter of gossiping tongues but through the language of electricity, where information pulses between

[18] (2012) 55 EHRR 2.

[19] Solove (n 4) 2.

massive record systems and databases".[20] Cyberspace and computers have widely increased our potentials to analyze, collect and store information. At present, it is observed that almost every entity, e.g., businesses, employers, government, and media are assembling information. Enumerable companies are maintaining digital-computerized records of their consumers' activities, preferences, and purchases. There are thousands of records about an individual's consumption, e.g., Amazon.com, an online retailer, is preserving records of the person buying books and other items, credit card companies are maintaining information regarding one's purchases using credit cards, etc.

In ***Boyd v United States***[21]**,** the Govt. wanted to coerce a merchant to the production of documents for use in a proceeding relating to civil forfeiture. The Court opined that the govt. could not forcefully disclose the dossiers because any compulsory and forcible extortion of a person's private papers or testimony to be used as a piece of evidence to forfeit his goods or to convict him of crime is a violation of his indefeasible right to private property, personal liberty and security.

Earlier, 'intrusion' was the only tool for collecting information or violating the right to privacy and other constitutional rights as well as human rights. However, nowadays, such intrusion or traditional eavesdropping or wiretapping is not always required as by dint of technological advancement, a person's privacy can easily be breached by using technological tools or by the tech companies.[22] For example, images (with personal details) were collected and communications made over personal Wi-Fi networks were intercepted by Google Streetview vehicles while mapping the landscape, and a lot of regulators and investigators found that the data encompassed completely identifiable personal information such as financial records and sensitive health data, as a result, Google faced various sanctions and paid fines in several jurisdictions.[23] In the same way, Snapchat was found to mislead its customers regarding a variety of data practices and the major breached contract was that the messages would 'disappear' permanently, which was a false statement, thus, Snapchat resolved the case with the Federal Trade Commission (hereinafter as "FTC").[24]

---

[20] ibid.

[21] 116 US 616 (1886).

[22] Tech Desk, 'Your Smartphone Could Be Recording Your Screen, Claims Study' (*The Indian Express*, 5 July 2018); available at:<https://indianexpress.com/article/technology/social/your-smartphone-could-be-recording-your-screen-claims-study/> accessed on 5 May 2020. See further, Warwick Ashford, 'Free Mobile Apps a Threat to Privacy, Study Finds' (*ComputerWeekly.com*) <https://www.computerweekly.com/news/2240169770/Free-mobile-apps-a-threat-to-privacy-study-finds> accessed on 5 May 2020.

[23] Electronic Privacy Information Center, 'Investigations of Google Street View' <https://epic.org/privacy/streetview/> accessed on 19 July 2020.

[24] 'Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False' (*Federal Trade Commission*, 8 May 2014) <https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were> accessed on 19 July 2020.

Moreover, The FTC observed that TRUSTe, an impressive provider of privacy trustmarks, was misrepresenting consumers in various ways which included untrue claims such as that was non-profit, certified corporations or companies belonged to definite data protection systems (such as the CORPA Safe Harbor or the EU-US Safe Harbor Framework), etc., and eventually, TRUSTe had to pay a U.S. $200,000 as 'disgorgement of profits' to fix the dispute.[25] It is observed that the US has not been applying the equitable philosophy of equity, justice and good conscience completely, however, the US is on a better footing to apply the equitable philosophy comparing to the EU.

4. Does the Right to Trade Trammel the Right to Privacy?

Prima facie it seems that the right to information and trade trammels or impedes the right to privacy. This proposition or speculation is not always true because in some substantial cases, without obtaining personal information, business attempts may go in vain.[26] That is why companies rely on various documents and evaluate their financial reputation. Earlier, the financial condition of a person can be traced easily by his/her appearance. In the modern age, it has become arduous to recognize a person's trustworthiness and estate. For these reasons, creditors generally rely upon the credit reporting agencies to accumulate information of an individual's credit history.[27] Such a credit report discloses the consistency of a person in paying back the debt incurred and the person's risk of being a loan defaulter.

Furthermore, the reports also contain liens, judgments, bankruptcy filings, outstanding debts, financial account information, and exhaustive financial history. Thus, a credit score is assigned to people which influences the decision-making as to whether they should be extended credit, and if the answer is in the affirmative, the amount of interests to be charged. The reports are of importance to secure a loan, get a job, rent an apartment, apply for a license, even to purchase a car or a home. Interestingly, information about a person's lifestyle and character is supplemented by investigative consumer reports prepared by credit reporting agencies.[28]

In ***Campbell v MGN Ltd.,***[29] a new methodology was introduced for the determination of entitlements for misapplication of private information. There are two phases in this method: (a) firstly, there is a threshold

[25] UNCTAD, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development', 52 <https://unctad.org/en/Publications...dtlstict2016d1_en.pdf> accessed on 9 July 2020.

[26] However, there are plethora of instances where the right to privacy is breached by unwarranted business actions. For example, see, note 11 and accompanying texts.

[27] Solove (n 4) 21.

[28] ibid.

[29] [2004] 2 AC 457, on appeal from: [2002] EWCA Civ 1373.

test, i.e., 'reasonable expectation of privacy'; (b) the second phase, i.e., 'the ultimate balancing test', is concerned with balancing the contending interests of privacy and freedom of expression in order to ordain which interest should prevail.

Lord Nicholls in ***Douglas v Hello! Ltd.***[30], stated that the misuse of confidential information or the breach of confidence now covers two distinct cases of action aimed at protecting two different interests, i.e., Privacy from one end and Secret (or confidential) information from another end. Information will be entitled to get protection in three circumstances: (a) first of all, when the information is (both) private and secret; (b) then whether the information is private but not secret, i.e., available in public domain; (c) last but not the least, whether the information is secret but not private, i.e., trade secret.[31]

It is vibrant that there will only be a reasonable expectation of privacy relating to information that is private to the claimant and which s/he did not anticipate to disclose, e.g., (a) information containing personal, business correspondence and accounts;[32] (b) personal financial and business information;[33] (c) political opinions;[34] (d) Personal appearances and image;[35] (e) Sexual orientation;[36] (f) Health and medical information; (g) Gender identification;[37] (h) Details of personal, intimate and sexual relationship;[38] (i) Information conveyed concerning such relationship;[39] (j) Information regarding a person's home and home life;[40] (k) Religious beliefs;[41] (l) Grief and emotional distress;[42] All the above-mentioned considerations are also backed by renowned case laws and discussing all the judge-made laws will exceed the ambit/periphery of the research, however, amongst the myriad judgments, a few are mentioned below.

4.1. Judge-made Laws Relating to Personal Financial and Business Information

In ***Browne v Associated Newspapers Ltd.,***[43] the Mail on Sunday desired to issue an article disseminating information about Lord Browne of Madingley – the then British Petroleum's (hereinafter as "BP") Group Chief Executive. The information impugned was provided to the newspaper by Jeff Chevalier who was the domestic

30 [2007] UKHL 21, [2007] 2 WLR 920.
31 ibid.
32 *Halford v UK* (1997) 24 EHRR 253.
33 *Browne v Associated Newspapers Ltd.* [2007] EWHC 2002.
34 *HRH Prince of Wales v Associated Newspapers Ltd.* [2006] EWCA Civ 1776.
35 *Von Hannover v Germany* (2005) 40 EHRR 1.
36 *Lustig – Pream v UK* (2000) 29 EHRR.
37 *Goodwin v UK* (2002) 35 EHRR 18.
38 *Applause Store Production Ltd. V Raphel* [2008] EWHC 1781.
39 *McKennitt v Ash* [2006] EWHC 3003.
40 *Beckham v MGN Ltd.* [2001] All ER (D) 307.
41 *Allause Store Production Ltd. V Raphel* [2008] EWHC 1781 (QB).
42 *Peck v UK* (2003) 36 EHRR 41.
43 [2007] EWHC 202 (QB).

partner of Lord Browne. The information encircled the following five types of subject matters: (a) the strategy of BP; (b) Lord Browne's wrong usage of the resources of BP and manpower to aid Mr. Chevalier; (c) the mere fact that the kinship between Lord Browne and Mr. Chevalier; (d) that Lord Browne disclosed secret BP matters and dossiers to Mr. Chevalier; and (e) relationships of Lord Browne with his colleagues at BP.

It was held that the above-mentioned considerations were subject to the reasonable expectation of privacy. The *ratio decidendi* was not for innately private information but due to the nature of the relationship and the circumstances of communication.

4.2. Case Laws Relating to Information Conveyed by Newspapers in the Context of Intimate Relationships

In *Theakston v MNG Ltd.*[44], a television and radio personality, Jamie Theakston, applied before the Court to obstruct the publication of an article in the Sunday People being Britain's one of the oldest Sunday newspapers disseminating the fact that the petitioner had visited a brothel situated in Mayfair, London and engaged with three prostitutes and detailed information regarding the intercourse, thereby, took place. It was held that such activity in a transitory relationship was not entitled to the same protection which could be availed by a comparatively more stable relationship, e.g., marriage.

A new approach, in this regard, had been applied in ***Mosley v News Group Newspapers Ltd.***[45], Max Mosley, the Federation Internationale de l'Automobile, sued the News of the World because of a published article dec=scribing Mosley's involvement at a sex party with five prostitutes and amongst them, one had sold her story to the newspaper. Hence, it was rendered that sexual encounters, however, could be considered under the umbrella of legitimate expectation of privacy.

In this ***Mosley*** case, story/information was sold to a newspaper and in the ***Theakston*** case, suit was initiated against another newspaper named Sunday People. Such incidents infer that right to trade can be thought identical to freedom of expression as in almost all the cases, it is being observed that the freedom of expression (while it is the case of a newspaper or tabloid) also encircles the right to trade. Therefore, the analogous philosophy/approach can be applied concurrently while dealing with disputes relating to trade and freedom of expression.

[44] [2002] EWHC 137 (QB).

[45] [2008] EWHC 1777 (QB).

5. International Laws Regulating Data Protection and Privacy

If we consider 'privacy' as a genus, then 'information privacy' is a species which refers to the accumulation of rules administering the assemblage and management of private data such as government and medical records, credit information, etc.[46] This sort of privacy is also known as "data protection" which is so crucial because, by the invasion of this category, horrible and pathetic experiences can be confronted by a person in cyberspace.[47] Nationally, the Republic of Bulgaria,[48] Kingdom of Denmark,[49] Republic of Estonia,[50] Republic of Hungary,[51] Republic of Poland,[52] Republic of Portugal,[53] Russian Federation,[54] Slovak Republic,[55] Republic of South Africa,[56] Kingdom of Spain,[57] Kingdom of Sweden,[58] etc. incorporated the provisions of 'information privacy' in their Constitutions.[59]

International human rights law acknowledges a person's privacy-related rights, notably Article 12 of the Universal Declaration of Human Rights, 1948 and Article 17 of the International Covenant on Civil and Political Rights, 1966 incorporate the provisions relating to the right to privacy and in Europe, the right to privacy is inserted through Article 8 of the European Convention on Human Rights (hereinafter as "ECHR") which forms a part of the constitutional application in European countries.[60] The member States must enact laws to make sure that the right to privacy, being a fundamental right, is enforced regarding the activities of private life as the ECHR has issued a ruling that member States are under an "obligation to give effect to the right to privacy under Article 8 of the ECHR".[61] The Council of Europe espoused Convention No. 108 in 1981 for the protection of persons relating to "Automatic Processing of Personal Data" and the ECHR mentioned that the protection of personal data fell under the ambit of the right to privacy as incorporated by Article 8 of the ECHR and, thus, the data protection enactments expanded quickly in the European countries throughout the 1990s.[62]

---

46 Md. Ershadul Karim, 'Citizen's Right to Privacy: Reflection in the International Instruments and National Laws' (2005) 9(1 & 2) Bangladesh Journal of Law 42.

47 ibid.

48 Constitution of Bulgaria 1991, Article 32.

49 Danish Constitution of 1953, Articles 71-72.

50 Constitution of Estonia 1992, Articles 42-44.

51 Constitution of the Republic of Hungary 1949, Article 59.

52 Constitutional Act 1997, Article 47.

53 Constitution of the Portuguese Republic 1976, Articles 26 and 35.

54 Constitution of the Russian Federation 1993, Chapter 2, Article 23.

55 Constitution of the Republic of Slovenia 1991, Articles 35 and 38.

56 Constitution of the Republic of South Africa 1996, Section 14.

57 Constitution of Spain 1992, Article 18.

58 Constitution of Switzerland 1874, Article 36(4).

59 Karim (n 46).

60 Irion, Yakovleva and Bartl (n 6) 3.

61 *Marckx v Belgium* [1979], ECtHR 6833/74, para. 31, regarding the right to respect for family life.

62 *Leander v Sweden* [1987], ECtHR 9248/81, para. 48.

6. Dispute Settlement Mechanism

The dispute settlement mechanism can be bifurcated into two heads. One is breach of privacy under national law and the other one is breach of privacy under international law. If the parties belong to the same nationality and the cause of action arises within the jurisdiction of the same state, then the dispute does come under purely national laws and jurisdictions. For example, in the case of Bangladesh, disputes of violation of privacy rights can be tried by the High Court Division (hereinafter as "HCD") of Bangladesh or can be tried by special courts or tribunals.[63] Furthermore, in the case of the EU and the US, the national jurisdiction includes the European Court of Human Rights (ECtHR) and FTC respectively.

Moreover, privacy laws in America are generally "caught in the gravitational orbit of liberty, while European law is caught in the orbit of dignity".[64] There are undoubtedly areas when the two entities of law approach one another more or less closely.[65] They are, so far, unswervingly pulled in diverse directions, and the outcome is that these (two) legal orders certainly do eloquently differ because continental Europeans are dependably more drawn to complications covering public dignity, whereas, Americans are considerably more drawn to complications touching on the destructions of the state.[66]

On the contrary, the conflict between different national privacy and international data flows standards has motivated two categories of international response: negotiation of trade rules, and cooperation between regulators.[67]

6.1. Negotiation

The ambit of the conflict between the right to trade and the right to privacy is not only limited to national affairs but also covers international affairs.

The General Agreement on Trade in Services (GATS) of the World Trade Organization (WTO) allows an exception for procedures required to secure conformity with laws. And those are not inconsistent with the GATS regarding privacy protection of individuals relating to the dispensation and dissemination of

---

[63] If we go through scholarly writings and leading case laws, we can find that (by interpreting Article 43 of the Constitution of People's Republic of Bangladesh) the right to privacy is considered as a fundamental right in Bangladesh and if a writ petition is filled regarding this issue, the High Court Division may issue rule in that regard under Article 102(2) of the Constitution. However, it is unlikely to have recourse to the HCD for the violation of information privacy affecting right to trade. Breach of privacy may also be entertained by special courts or tribunals backed by other laws such as the Information and Communication Technology Act 2006, the Digital Security Act 2018, etc.

[64] James Q Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113(1151) The Yale Law Journal 1163.

[65] ibid.

[66] ibid.

[67] Mattoo and Meltzer (n 10).

personal or private data.[68] The essence of Article XIV restricts the exception to procedures that do not lead or guide to unjustifiable and unnecessary discrimination among countries where identical conditions prevail.[69] While the WTO appellate body and panels "have made judgments in other cases on whether" an initiative was required to attain a definite objective, it is almost certainly unrealistic to expect an already strained dispute management system of WTO to deliver judgment on the politically sensorial issue of privacy protection.[70] The WTO's Dispute Settlement Body (DSB) or appellate body, whatever the case may be, should apply the principle of 'inter-operational equity' instead of following the very words (or literal rule of interpretation) in cases where there are chances to create ambiguity or where the judgment based on the very words of law imposes unwarranted hardship to any of the parties.

7. Regulatory Co-operation

It can be thought of as a hybrid form of Alternative Dispute Resolution (hereinafter as "ADR"), e.g., Med-arb (a combination of mediation and arbitration, Reg-neg (regulatory negotiation), etc. Moreover, it is a well-known principle (by renowned jurist Thomas Erskine Holland) that "International law is the vanishing point of jurisprudence". A state consists of a particular and identifiable territory, sovereignty, its people and government. The word "sovereignty" includes, *inter alia*, the ability to enter into a contract with other authorities. The sovereignty of a State can hardly be determined by hard and fast customs and rules. That is why the influence of various forms of ADR in international law is lucidly observed. Customarily regulatory co-operation implies mutual recognition and harmonization which is improbable in this case and would not be adequate to guarantee international flows of data.[71] Mutual recognition and harmonization of national laws and regulations assist firms to form "economies of scale" as it is not required to differentiate operations to conform to conflicting regulations.[72] However, identical and/or mutually acceptable laws and regulations do not address the vital problem of international data flows.[73] While conducting regulatory co-operation or any type of hybrid forms of ADR, the application of the 'inter-operational equity' principle may provide more effective outcomes.

[68] WTO Analytical Index, GATS – Article XIV (Jurisprudence), Article XIV(c) <https://www.wto. org/english/res_e/publications...gats_art14_jur.pdf> accessed on 27 December 2020.

[69] Mattoo and Meltzer (n 10).

[70] ibid.

[71] ibid.

[72] ibid.

[73] ibid.

8. Conclusion

A firm, corporation, or company, whatever the case may be, conducting its works or business nationally or internationally, should collect and/or supply only the very information which is required for complying with the conditions incorporated in the memorandum of understanding, keeping in mind that a contract dealing with illegal goods or items or things (as in this case, illegal data or information) is void and such contract is not enforceable by any court of law.

Trade should be conducted without any kind of violation of one's right to privacy. The state, legislature and law enforcement authorities should remain vigilant so that no one's right to privacy is breached. Trade facilitators should take initiatives so that the traders or tech companies cannot even think of the breach of privacy rights. As it is not practical to expect the incorporation of 'equity' in all laws in a short span, therefore, the judges or respective authorities should not render judgment based on the very words of laws rather the authorities should pronounce judgment on the intent and philosophies thereof. The *Respondeat Superior* rule ought to be applied so that principal (in this case, the 'employer') shall be responsible for the acts done by his/her agent (in this case, the 'employee'). Furthermore, if traditional dispute settlement mechanisms fail to operate, hybrid forms of ADR may be introduced keeping in mind the facts and gravity of the circumstances. Reg-neg or Negotiated rule-making may be a decent example in this regard.

It is prominent that customary rules or conventional laws (and procedures) can neither strike a balance between trade and privacy nor such laws can shield the privacy of the citizens by incorporating effective laws or by enforcing existing laws. Thus, the application of equity and good conscience becomes obvious. Hence, all persons (including both natural and artificial persons) should be held accountable for violating one's right to privacy by transmitting illegal data for business purposes. The regulators and policymakers in each country should influence the performance of data-handling entities (situated within or outside their jurisdictions) to shield the interests of their citizens.[74] As human rights are indivisible, all rights should be given the same importance and legal effect and if any conflict arises while enforcing these rights concurrently, a balance should be taken place based on equity and the gravity of the circumstances. Today there is no operation of the Judicature Act of 1873 and the Court of Equity or Court of Chancery is not in existence, however, the essence of equity is inherent in almost every statute.[75] Therefore, equilibrium should be made (by applying the philosophy of 'equity') in the same way it ought to be taken place between freedom of expression or right to information and right to privacy or right to property or trade secrets.

[74] Mattoo and Meltzer (n 10).

[75] Ahmad (n 1).