DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4189

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

CRITICAL ANALYSIS OF DIVERGENT APPROACHES TO PROTECTION OF PERSONAL DATA

Sandeep Mittal
Cyber Security & Privacy Researcher
Former Director, LNJN NICFS (MHA)
New Delhi, India

Abstract: The protection of privacy and confidentiality of personal data generated on internet at residence and in motion within and across the border is a cause of concern. The European Union and United States have adopted divergent approaches to this issue mainly due to varying socio-cultural backgrounds. With the globalisation of businesses facilitated by internet revolution, the economic considerations out-weighed the rights consideration, and the right based approach started buckling the pressure of economic based approach but was checked by the Schrem's case. The negotiation under TTP and TTIP has a tendency to forgo the privacy rights of the individuals over business considerations in tune with the US tactics of weakening the privacy laws through Free Trade Agreements. It has been demonstrated that a balanced approach in which individual control over data is desirable but should not be absolute, control rights are reinforced by structural safeguards or architectural controls would be desirable.

Keywords: Personal Data; Internet Governance; Right to Privacy***;*** Data Privacy Protection; Trans-Pacific Partnership (TPP); Transatlantic Trade and Investment Partnership (TTIP**);** Protection of Privacy;

I. INTRODUCTION

The number of Internet users in the world has increased by 826 per cent, from 16 million in 1995 to 3,270 million in the last 15 years, accounting for about 46 per cent of the world population. [1] The Internet has emerged as a preferred medium of expression of free speech, conducting trade and business, and running daily errands like controlling multipurpose home devices, thereby generating large volumes of personal data. This data includes names, addresses, mobile numbers, dates of birth, emails, geographical locations, and health records like the BMI and can aid in advertising for marketing purposes. Internet users access the Internet through an 'Internet Service Provider' (ISP), who provides infrastructure, allowing users to access the Internet and user-generated content. This big data, which has been disclosed voluntarily or incidentally through interactive means (for example, Online Surveys) or technological (for example, Cookies) has a high potential for secondary uses. The right of privacy in general is "the right of the individual to be left alone; to live quietly, to be free from unwarranted intrusion to protect his name and personality from commercialisation." [2] [3] The protection of privacy and confidentiality of this personal data at the residence and in motion within and across the borders is a cause for concern, [4] [5] [6] [7] more particularly in the developed economies like the European Union (EU) and the US. The EU and US have adopted divergent approaches [8] [9] [10] [11] to this issue. The scope of this essay is to critically analyse these comparative but divergent approaches for protecting privacy.

II. THE EUROPEAN UNION APPROACH

The basic premise of the EU privacy protection approach is embodied in the EU Directive 95/46, [12] recognising privacy as a fundamental human right as demonstrated by the repetition of the term 'fundamental right and freedom' 16 times in the Directive. Para 10 of the adoption statement of the Directive states,

"Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;" [13]

The Directive 1995/46 [14] gives far-reaching powers and complete control over personal data to individuals, thus creating severe legal issues not only for domestic and international businesses but also for sovereign nations in dealing with personal data. [15] The basic framework of this Directive is summarized [16] as follows:

a) Companies to inform users regarding their policy in handling the personal data collected from them.
b) Affirmative consent of users to be obtained to collect, use, and disseminate the data.
c) Documentation and registration of the above consent with 'data authorities', who would retain the data in their own databases.

d) Accessibility of the database to individuals for amendments and/or rectifications in their data.
e) Identity of the companies collecting the data to be disclosed to the consumers.
f) Explicit bar on trans-border data transfer if the laws destination country lacks adequate data protection.

The spirit of fundamental rights has been further reiterated and refined in the EU Directive 2002/58/EC [17]. This Directive prohibits any type of interception or surveillance, erasure and anonymisation of processed data and location-related data, an opt-out regime for itemised-billing and calling-line identification. Most importantly, inclusion of the opt-in regime for cookies [18] needs to be stored in the browser, with all these conditions being subject to consent, with certain exceptions like security or criminal acts.

The 'consent' in the 2002 Directive has been replaced with 'informed consent' in the Directive 2009/136/EC.[19] Recently, the EU passed Regulation (EU) 2016/679, which would replace the existing privacy law in the EU by 25 May 2018. It is a comprehensive regulation covering businesses outside the EU, with the data too residing outside the EU. It has also incorporated provisions regarding the custodian's explicit informed and verifiable consent for children below 13 years of age, and penalty up to 4 per cent of the global business annual turnover of the preceding financial year, in case of violation of privacy. Thus, the approach of the EU to protect the privacy of an individual essentially remains 'regulatory, State-controlled and penal' and devoid of self-management. [20] [21] [22] [23]

III. THE US APPROACH

The US approach to the protection of online privacy is 'self-regulatory', favouring voluntary market-based approaches over central regulation depending mainly on industry norms, and codes of conduct, among other things. The laws are in piece-meal form, sporadic, inadequate or non-existent, demonstrating that the protection of privacy is not an issue for the political and democratic systems in the US. [24] Most of the privacy provisions in various US Acts like The Driver's Privacy Protection Act of 1984, the Video Privacy Protection Act of 1988, The Electronic Communications Privacy Act of 1986, and The Cable Communications Policy Act of 1984 are akin to knee-jerk reactions to public scandals and outcries.[25] [26] There is neither a comprehensive law nor any comprehensive mechanism to enforce the protection of privacy in the US, leaving everything to 'industry self-regulation'.[27] However, due to the interdependence of EU-US businesses over each other and the presence of a well-crafted law in the EU, there is a tendency among US companies to draft some kind of a voluntary code for data protection, which would act as a 'privacy-protection face-mask' to purport as having respect for privacy protection, on the one hand, and as a smoke-screen to keep the government regulation at bay, on the other. Even the US negotiated 'Safe Harbour Privacy Principles' as an alternative to the adequacy clause in Article 25 of Directive 95/46/EC, wherein US businesses qualifying as 'safe harbours' would be deemed to have provided adequate privacy protection. [28] This 'safe-harbour' concept is a self-certifying framework mechanism based on seven principles,[29] as enumerated below:[30]

a) Notice to individuals regarding the likely uses of their data and the mechanism available to them for complaint and grievance redressal.
b) 'Opt-out' choice to individuals with regard to the collection of data and its dissemination to third parties.
c) Transfer of data only to third parties having adequate privacy protection.
d) Reasonable security assurance measures to prevent the loss of collected information.
e) Measures to ensure the integrity of data.
f) Accessibility of data to individuals for correction or deletion of incorrect data.
g) Enforcement mechanism for these guidelines.

However, there is little or no regulation by the Government except the 'safe harbour registration, on payment of a nominal fee and the guidelines' implementation is self-certified through either trained employees or through private industry-funded bodies. For example, TRUSTe investigates the companies that provide funding to it, thus inviting criticism. [31] The 'safe harbour' provision was struck down as invalid [32] by the Court of Justice of the European Union in 2015 as below,

"1. Article 25(6) of Directive 95/46/……. as amended by Regulation (EC) No 1882/2003….., read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.
2. Decision 2000/520 is invalid." [33]

Subsequently, in view of the invalidation of the 'safe-harbour framework' and Regulation (EU) 2016/679 [34] likely to be in place by mid May 2018, with provisions of heavy penalties of up to 4 per cent of the international annual turnover during the preceding financial year, the US Government has negotiated an "EU-U.S. Privacy Shield" with the European Commission, which is purportedly more stringent and robust than the 'safe harbour framework'.[35] In future, the US would bring pressure upon the EU to include the privacy

protection framework while negotiating the TTIP, but the EU would have to limit itself within the framework prescribed by the CJEU.[36] [37] [38]

IV. THE EU APPROACH VERSUS THE US APPROACH

While the EU approach recognises the protection of privacy as a fundamental human right, the US approach is to adopt an iota of interference in the privacy rights of individuals, treating these rights as a commodity, thus leaving the issue to market forces as stated by scholars.[39] [40]

"The US approach contrasts the EU approach to data privacy. [41] Whereas in the EU, it is the responsibility of the government to protect citizens' right to privacy, in the U.S., markets and self-regulation, and not law, shape information privacy. In the EU, privacy is seen as a fundamental human right; in the U.S., privacy is seen as a commodity subject to the market and is cast in economic terms David Aaron, who negotiated the Safe Harbor, noted that in Europe: Privacy protection is an obligation of the state towards its citizens. In America, we believe that privacy is a right that inheres in the individual. We can trade our private information for some benefit. In many instances Europeans cannot. This can have important implications when it comes to e-commerce."[42]

Does this statement give an impression that the US has closed its eyes to the stringent data privacy laws in the EU? Superficially, it may appear so but that is only an illusion. The US is vigorously using its negotiating skills in drafting Free Trade Agreements (FTAs) with trading partners across the globe, incorporating crippling provisions, putting fetters on the data privacy concerns, in the name of facilitating free trade. Disguised in this is the message that if a partner wants free trade with the US, its data privacy laws should not act as impediments to the free flow of data to the US. Two such FTAs of interest are the Trans-Pacific Partnership (TPP), which has already been signed but is not in force, and the Transatlantic Trade and Investment Partnership (TTIP) being negotiated between the EU and the U.S. in secrecy, wherein the U.S. has well-intentioned moves to soften the relatively stringent privacy law, thus giving a protection shield to US businesses from prosecution under the 'post-SchremEU Law' [43]. The TTIP is under negotiation, but the intentions of the US with regard to the protection of privacy are obvious in the TPP agreement.

The TPP is the first legally binding international agreement affecting data privacy, with provisions for the enforcement of violations. "The TPP only imposes the most limited positive requirements for privacy protection, but imposes stronger and more precise limits on the extent of privacy protection that TPP parties can legally provide."[44] Let us take a peep into the TPP's provisions affecting data security, as enumerated in Table 1. [45] [46] [47]

A perusal of the TPP's provisions, as delineated in Table 1, would send a 'chill wave' down the spines of proponents of data protection privacy. The entire exercise seems to be an attempt by the US to by-pass the local data privacy laws to protect businesses operating from its soil and to pre-empt litigation against its own business interests. The vigour with which the US is pursuing these FTAs is evident from the passage of the Trade Promotion Authority Bill by the Senate, which was termed as ".....an important step toward ensuring [that] the United States can negotiate and enforce strong, high- standards trade agreements....." by the US Presiden [48]

Table 1: Effects of TPP on Data Privacy Protection [49] [50] [51]

S. N.	TPP Article	Brief Title	How it affects Data Privacy
1.	14.2.2 14.2.4	Scope includes any measures affecting trade by electronic means	a) Scope is much wider as it applies to measures affecting trade (not limited only to measures governing or applicable to trade) by electronic means (not limited only to electronic commerce). Thus the scope is much wider than it looks. b) Measures affecting the supply of service performed or delivered electronically are subject to obligations contained in relevant articles of Chapters 9 (Investment), 10 (Cross-Border Trade in Services) and 11 (Financial Services).
2.	14.8	Vague & unenforceable Requirements for Protection of personal information	a) Obligation on parties to provide legal framework for the protection of personal information of the users of electronic commerce only. Not applicable if electronic commerce not involved. b) No mention of protecting information as protecting human rights. c) 'Measure is defined to include a 'practice' or 'law', thereby implying that even legal framework is given a go-bye to include 'self-regulation' practice in U.S. (Article 1.3) d) Parties free to adopt different legal approaches but should encourage cross-border compatibility which is left vague with no standards or mechanism of enforcement included. e) Party shall endeavour to adopt non-discriminatory

			practices to provide data privacy protection would mean that this would not be limited only to citizens but equally to non-residents also.
3.	14.11	Restrictions on data export limitations	a) Each party may have its own regulatory requirements regarding transfer of information by electronic means and may allow cross-border transfer of data if it pertains to business of a service suppliers from one of the TPP Parties. Any exceptions to this would have to be justified by applying four requirements of Article 14.11.3 as follows, (i) Legitimate public policy Objective. (ii) Not an arbitrary or unjustifiable discrimination. (iii) Not a disguised restriction on trade. (iv) Restrictions imposed on transfer of data not greater than that required to achieve the objective. Onus of burden to prove Clauses (ii) and (iii) above would lie on party imposing the restrictions.
4.	14.13	Ban on data localisation	a) A TPP Party Service supplier is not required to use computing facilities or data localisation facilities in the territory of a TPP Party where he want to conduct business. b) In case of any exception, the four-step test of data export limitations.
5.	28	Complex Dispute Settlement Procedures	The dispute settlement procedures are lengthy and complex and could even lead to revoke the benefits under free trade.
6.	9	Investor-State Dispute Settlement (ISDS)	An investor from one party in territory of other party must be accorded for dispute settlement purpose, a) 'National Treatment' b) 'Most-Favoured-Nation Status' & c) Fair and equitable treatment d) Full protection and security e) Prohibition of direct or indirect expropriation of investment except for public purpose or fair compensation.

A study of the TTIP Text, [52] which was being negotiated in secrecy, reveals that privacy concerns are being sacrificed over so-called free trade. The salient features of the privacy provisions are as follows: [53]

a) Article 33(2) provides for only 'adequate safeguards' and 'not legislation' for protection of privacy, and is thus very mild.
b) Article 33(1) provides unrestricted cross-border transfer of personal data for providing financial services.
c) Article 7(1) provides general exceptions exempting measures for protecting the privacy of personal data subject to three qualifications, [54] that the measures:
   (i) must be necessary,
   (ii) must not constitute 'arbitrary or unjustifiable discrimination between countries where like conditions prevail', and
   (iii) must not be 'a disguised restriction on establishment of enterprises, the operation of investments or cross-border supply of services'.

It remains to be seen how the two contrasting approaches to the protection of privacy culminate into each other in the name of free trade. The rights-based approach is getting crushed under the growing weight of the economics-based approach being adopted by the combined might of the EU-US nexus.

V. CONCLUSION

The varying cultural backgrounds of the societies of the EU and US were initially reflected in their contrasting approaches to the protection of privacy. With the globalisation of businesses facilitated by the Internet revolution, the economic considerations out-weighed the rights considerations, and the rights- based approach started buckling under the pressure of the economics-based approach. However, the Schrem's case put a brake on this tendency. The EU may be reminded that it cannot negotiate the privacy rights of individuals. However, the TTIP text discloses the position of the EU on privacy protection. This stance of EU is not very conducive to the protection of privacy. They seem to be eager to forego the privacy rights of individuals over business considerations in tune with the tactics adopted by the US to weaken the privacy laws through FTAs. Recent developments like BREXIT, the trade expansionist policy followed by the US and the probable future dependence of the EU on the US for its economic survival and stability would decide if these two comparative and contrasting approaches to the protection of privacy would remain so or would evolve into a 'willingly-accepted-forced' compromise by sacrificing the privacy rights of individuals. What is desirable is a balanced approach in which individual control over data is desirable but not absolute, control rights are reinforced by structural safeguards or architectural controls, and self-management is possible [55] for protecting privacy in an age of voluntary disclosure and secondary uses of personal data.

VI. REFERENCES

[1] M. M. Group. (2015, 24.11.2015). World Internet Users Statistics and 2015 World Population Stats. Available: http://www.internetworldstats.com/stats.htm

[2] A. Lindey, Lindey on Entertainment, Publishing, and the Arts: Agreements and the Law vol. 2: C. Boardman Company, 2005.

[3] S. Sorensen, "Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights," Child. Legal Rts. J., vol. 36, p. 156, 2016.

[4] S. R. Salbu, "European Union Data Privacy Directive and International Relations, The," Vand. J. Transnat'l L., vol. 35, p. 655, 2002.

[5] J. Kang, "Information privacy in cyberspace transactions," Stanford Law Review, pp. 1193- 1294, 1998.

[6] J. P. Graham, "Privacy, computers, and the commercial dissemination of personal information," Tex. L. Rev., vol. 65, p. 1395, 1986.

[7] D. H. Flaherty, "On the utility of constitutional rights to privacy and data protection," Case W. Res. L. Rev., vol. 41, p. 831, 1990.

[8] J. M. Assey Jr and D. A. Eleftheriou, "EU-US Privacy Safe Harbor: Smooth Sailing or Troubled Waters, The," CommLaw Conspectus, vol. 9, p. 145, 2001.

[9] D. R. Nijhawan, "Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States, The," Vand. L. Rev., vol. 56, p. 939, 2003.

[10] J. R. Reidenberg, "E-commerce and trans-atlantic privacy," Hous. L. Rev., vol. 38, p. 717, 2001.

[11] D. Zwick and N. Dholakia, "Contrasting European and American approaches to privacy in electronic markets: property right versus civil right," Electronic Markets, vol. 11, pp. 116-120, 2001.

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281 , 23/11/1995 P. 0031 – 0050 (Accessed at: http://www.refworld.org/docid/3ddcc1c74.html on 14 November 2016), 1995.

[13] ibid. paras 1, 2, 10 and art 1, para1.

[14] ibid.

[15] J. S. Bauchner, "State sovereignty and the globalizing effects of the Internet: A case study of the privacy debate," Brook. J. Int'l L., vol. 26, p. 689, 2000.

[16] D. R. Nijhawan, "Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States, The," Vand. L. Rev., vol. 56, p. 939, 2003.

[17] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Official Journal of the European Union, Vol. L 201 (2002), pp. 0037-0047 by European Parliament and the Council of the European Union (Accessed at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058 on 14 November 2016), 2002. Recital 1,2,3 and 11.

[18] ibid. Recitals 24, 25, art 5(3)

[19] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) OJ L 337, 18.12.2009, p. 11–36, 2009. Art 3 (5).

[20] F. Giampaolo, "Overview of the main topics of EU Regulation 2016/679-General Data Protection Regulation."

[21] F. Mauro and D. Stella, "Brief Overview of the Legal Instruments and Restrictions for Sharing Data While Complying with the EU Data Protection Law," in International Conference on Web Engineering, 2016, pp. 57-68.

[22] M. Boban, "DIGITAL SINGLE MARKET AND EU DATA PROTECTION REFORM WITH REGARD TO THE PROCESSING OF PERSONAL DATA AS THE CHALLENGE OF THE MODERN WORLD," in Economic and Social Development (Book of Proceedings), 16th International Scientific Conference on Economic and Social, 2016, p. 191.

[23] H. Kranenborg, "O. Lynskey, The Foundations of EU Data Protection Law," ed: Oxford University Press, 2016.

[24] F. H. Cate, "Principles of Internet Privacy," Conn. L. Rev., vol. 32, p. 877, 1999.

[25] G. Shaffer, "Globalization and social protection: the impact of EU and international rules in the ratcheting up of US data privacy standards," Yale Journal of International Law, vol. 25, pp. 1-88, 2000.

[26] J. R. Reidenberg, "E-commerce and trans-atlantic privacy," Hous. L. Rev., vol. 38, p. 717, 2001.

[27] S. Listokin, "Industry Self-Regulation of Consumer Data Privacy and Security," J. Marshall J. Info. Tech. & Privacy L., vol. 32, p. 15, 2015.

[28] J. M. Assey Jr and D. A. Eleftheriou, "EU-US Privacy Safe Harbor: Smooth Sailing or Troubled Waters, The," CommLaw Conspectus, vol. 9, p. 145, 2001.

[29] Safe Harbor Framework Overview available at, https://build.export.gov/main/safeharbor/eu/eg_main_018476 (Accessed 15 November 2016)

[30] Original documents can be retrieved at, http://webarchive.loc.gov/all/20150405033356/http%3A//export.gov/safeharbor/eu/eg_main_018493.asp (Accessed on 15 November 2016)

[31] G. Shaffer, "Globalization and social protection: the impact of EU and international rules in the ratcheting up of US data privacy standards," Yale Journal of International Law, vol. 25, pp. 1-88, 2000.

[32] "Maximillian Schrems v Data Protection Commissioner, C-362/14, Court of Justice of the European Union," ed: Court of Justice of the European Union 2015. Accessed at, http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=en (Accessed on 15 November 2016)

[33] ibid.

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88 2016.

[35] EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce. (2016) Accessed at, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf (accessed on 15 November 2016).

[36] D. Bender, "Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective," International Data Privacy Law, p. ipw005, 2016.
[37] L. J. Sotto and C. D. Hydak, "The EU-US Privacy Shield: A How-To Guide," Law360, pp. 1-4, 2016.
[38] M. A. Weiss and K. Archick, "US-EU Data Privacy: From Safe Harbor to Privacy Shield," Congressional Research Service, 2016.
[39] S. J. Kobrin, "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance," Review of International Studies, vol. 30, pp. 111-131, 2004.
[40] L. B. Movius and N. Krup, "US and EU privacy policy: comparison of regulatory approaches," International Journal of Communication, vol. 3, p. 19, 2009.
[41] S. J. Kobrin, "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance," Review of International Studies, vol. 30, pp. 111-131, 2004.
[42] L. B. Movius and N. Krup, "US and EU privacy policy: comparison of regulatory approaches," International Journal of Communication, vol. 3, p. 19, 2009.
[43] "Maximillian Schrems v Data Protection Commissioner, C-362/14, Court of Justice of the European Union," ed: Court of Justice of the European Union 2015.
[44] G. Greenleaf, "The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy?," Available at SSRN 2732386, 2016. Accessed on 20/11/2016 at, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732386&download=yes
[45] ibid.
[46] B. K. T. Israel. (2015, The Highlights of the Trans-Pacific Partnership E-commerce Chapter. Accessed at http://www.citizen.org/documents/tpp-ecommerce-chapter-analysis.pdf on 20/11/2016.
[47] G. Greenleaf, "International Data Privacy Agreements after the GDPR and Schrems," 2016.
[48] "Statement by the President on Senate Passage of Trade Promotion Authority and Trade Adjustment Assistance," ed. Washington DC: The White House, 2015.
[49] B. K. T. Israel. (2015, The Highlights of the Trans-Pacific Partnership E-commerce Chapter. Accessed at http://www.citizen.org/documents/tpp-ecommerce-chapter-analysis.pdf on 20/11/2016.
[50] G. Greenleaf, "The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy?," Available at SSRN 2732386, 2016.
[51] G. Greenleaf, "International Data Privacy Agreements after the GDPR and Schrems," 2016.
[52] TTIP Text available at http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf (Accessed on 20/11/2016)
[53] G. Greenleaf, "The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy?," Available at SSRN 2732386, 2016.
[54] TTIP Text available at http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf (Accessed on 01/12/2016)
[55] H. Kranenborg, "O. Lynskey, The Foundations of EU Data Protection Law," ed: Oxford University Press, 2016.

