

## GOOGLE, THE BEST ICT BUSINESS MODEL OR THE WORST EVIL LAW EVER FACED

Tossapon Tassanakunlapan

Faculty of Law, University of Barcelona. Law Lecturer at Chingmai University, Thailand.

---

### ABSTRACT

*Google is the prominent ICT Corporation who launched vast majority inventive products and services into information market. Thus Google has come to legal scholar concerns since they have launched multiple tasks to fulfill users' demands. Some applications such as Google search engine, Google Chrome web browser and Google visual map make a critical impact on individual rights directly and indirectly. These applications invented and developed by ongoing data processing. However, they have claimed to society that 'Google does no evil'.*

*The prominent book 'Google and the Law; Empirical Approaches to legal aspects of knowledge-economy business models' addresses various effects Google brings to legal atmosphere. Nonetheless, the vital issue on data processing and data mining are missed out. Howbeit, the efficiency of governance models on Internet Service Providers (ISPs) is relevant with diverse conditions. In different States and Regions, The design and implementation of regulatory regime are significant conditions.*

*Google is the recently new mega power in information-based society which could provide various services to a vast majority of internet surfers and turn users into their products by data processing. However, the penetration and collection of personal data by Google are unpredictable high and deep in long run. The inquiry on the individual rights protection during the data processing and the legitimacy to use it still remain. The prospect article would clarify if States and Regional regimes have been brought to tackle the problems. Ultimately, the article result could be extracted to formulate an embedded ISPs regulation on data protection in international, regional and domestic level.*

*Under Google influence, they handle nearly two-thirds of Internet search queries worldwide that most web sites rely on the search engine for half of their traffic. When Google engineers twist its algorithm, they can break the business of a Web site by decreasing their rankings. In this model, States will lessen power over the online, but the government can embed power into the technical architecture of the Internet itself if they want in that specific strict "Zone", which will be described in various models.*

*Key Words: Google, Personal Data Protection, Cyber Regulation, International Regime, ICT Corporation, Data Processing, E-Commerce, Information*

---

### Background and Rationale

At First, there are obviously needs of business to improve their capacity to operate in New Informative Market, E-Commerce Society. Furthermore, The Corporation prefers a wide open Market Society for freedom on commercial activities. For accomplish their goal, the Private Sector has been proposing for less State intervention in order to boost the creativity to invent new products. The new products and services in forthcoming market are Information and Communication Technology (ICT)'s off springs which have been invented by employing various forms of data processing services. Moreover, Governments have been stimulated by private sectors to reform their efficiency and save corporate cost on processing Personal Data. Hence, there is an evident on the 'unavoidable' economic and social conditions which could be proved by the economic figures<sup>1</sup> that Western States must support their private sector to generate more productivity in a time of Economic Collapse.

Google is the prominent ICT Corporation who launch vast majority inventive products and services into information market. Thus Google has come to legal scholar concerns since they have launched multiple tasks to fulfill users' demands. Some applications such as Google search engine, Google Chrome web browser and Google visual map make a critical impact on individual rights directly and indirectly. These applications invented and developed by ongoing data processing. However, they have claimed to society that 'Google does no evil'.<sup>2</sup>

The prominent book 'Google and the Law; Empirical Approaches to legal aspects of knowledge-economy business models'<sup>3</sup> addresses various effects Google brings to legal atmosphere. Nonetheless, the vital issue on data processing and data mining are missed out. Howbeit, the efficiency of governance models on Internet Service Providers (ISPs) is relevant with diverse conditions. In different States and Regions, The design and implementation of regulatory regime are significant conditions.

Google is the recently new mega power in information-based society which could provide various services to a vast majority of internet surfers and turn users into their products<sup>4</sup> by data processing. However, the penetration and collection of personal data by Google are unpredictable high and deep in long run. The inquiry on the individual rights protection during the data processing and the legitimacy to use it still remain. The prospect article would clarify if States and Regional regimes have been brought to

---

<sup>1</sup> R Towey, 'Internet contribution to UK economy down to e-commerce', <<http://www.peer1hosting.co.uk/industry-news/internet-contribution-uk-economy-down-e-commerce>>, accessed on 1 November 2012.

<sup>2</sup> Google, Google Motto in internal corporate meeting 2001 on the theme "What Google was all about", 2001.

<sup>3</sup> A Lopez-Tarruella, 'Introduction: Google pushing the boundaries of Law', *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, T.M.C. Asser Press, Hague, 2012, p.4-5.

<sup>4</sup> V T Siva, *THE GOOGLIZATION OF EVERYTHING : (AND WHY WE SHOULD WORRY)*, University of California Press, Berkeley, 2011, p.3.

tackle the problems. Ultimately, the article result could be extracted to formulate an embedded ISPs regulation on data protection in international, regional and domestic level.

Under Google influence, they handle nearly two-thirds of Internet search queries worldwide that most web sites rely on the search engine for half of their traffic. When Google engineers twist its algorithm, they can break the business of a Web site by decreasing their rankings. In this model, States will lessen power over the online, but the government can embed power into the technical architecture of the Internet itself<sup>5</sup> if they want in that specific strict "Zone", which will be described in later models. The regulation of Cyberspace could be apply by some others Service Sector market governance. The ICT Regulation which may mentioned to clear up the idea are Co-Regulation, Multi-Layer, Poly-Centric Model for regulate the ISPs on Personal Data Processing.

As The ICT Corporations are the leading actors in this dilemma of Data Processing and Data Protection issue, the relationship between Internet Service Providers (ISPs) and Internet Users are crucial to analysis. The threats to personal data protection posed by non-state actors, in this case the Google Corporations, is the amassing huge stores of searchable data they have possessed. They cumulate Big Data by using the 'Compulsory Consent terms and Conditions' model. This contract of application form is usually used by ISPs to address issues of data privacy. Nonetheless users are given 'freedom of choice' to opt in to or opt out of data collection activities<sup>6</sup> without reading the Terms and Conditions for using such services carefully.

Due to the competence of Google on the basis of Technology Determinism which is driven by market, the importance of cyberspace governance have been highly recognized in the model of State-Regulation<sup>7</sup> but they are still questioned about the balancing of power that whether let the authority do it all or some checks and balances should be prevailed. However, too much interference would deter the creativity to develop private sectors.

The issue on Moral Hazard problems of Relationship between individual rights and public order should be raised. The answer might be the balance of control to shift the boundary between those two and the Governance Model for Regulating ISPs and Protecting Individual rights. The problems here is what state must do and what must be done by private without state over-interfering.

Moreover, the article may explore the cooperation or conspiracy among states and ISPs. It seems to be sure that Google Corporation has a power over personal data processing. People will never know whether they share it with government or not. Google usually share personal data and information with state agencies<sup>8</sup> which consistently exchange the information on political basis and Google gain economical benefit in return.

Ultimately, are just the internet surfers who really use Google? On the contrary, state especially government and security agencies do processing, mining and sharing the information with Google.<sup>9</sup> The orthodox excuses of the state are; to support the flourishing of economy and protect National Security<sup>10</sup> which is vague and undermine the fundamental rights of individual as a customer and people.

The historical background of data processing and protection problems require understanding on both State and Human Security perspectives.<sup>11</sup> Not only political and economic conditions but also social and cultural principles as well.

After the end of Cold War Era, the race to proliferate Strategic weapons of mass destructive among Super power Countries has been decreasing. Due to the high expenses and risk that threat the International Security, the competition on WMD proliferation had been transformed to new strategic plan.<sup>12</sup> The old proliferation of such physical weapons has been turned to the new safer and better image strategy. The Secret collection of Intelligences via Information and Communication Technology<sup>13</sup> is the latest secret weapon that USA chose to employ as weapons in a time of hot peace. Since the development of Internet at first place was base on Military use,<sup>14</sup> the more technology advantage US ISPs are the more power the US Intelligence get. The most advantage US has is the commercial development of ISPs that provide various applications and service to diverse peoples all around the world. The turning point from WMD proliferation on physical space to intelligence collection on cyber space has generated the problems and discontents. (Military Interest)

<sup>5</sup> J Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors', *University of Cincinnati Law Review*, 66, 1997, extracts from pp. 177–205.

<sup>6</sup> J E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object', *GEORGETOWN LAW The Scholarly Commons*, 2000, p.1373–1438.

<sup>7</sup> L E Bygrave, J Bing, *Internet Governance: Infrastructure and Institutions*, Oxford University Press, Oxford, 2011, p. 70-71.

<sup>8</sup> M Ingram, Google publishes figures on government requests for data, *World Socialist Website*, <<http://www.wsws.org/articles/2010/apr2010/goog-a26.shtml>>, accessed on 31/10/2012.

<sup>9</sup> \_\_\_\_\_, \_\_\_\_\_, <<http://www.google.com/transparencyreport/userdatarequests/faq/>>, accessed on 31 October 2012.

<sup>10</sup> Article 9(2)(a) of Strasbourg Convention 1981.

<sup>11</sup> M C Kettmann, *The Future of Individuals in International Law: Lessons from International Internet Law*, eleven international publishing, Hague, 2013, Extract.

<sup>12</sup> Y Aubin, A Idiart, (eds), *Export Control Law and Regulations Handbook: A Practical Guide to Military and Dual-Use Goods trade restriction and compliance*, Kluwer Law International, Netherlands, 2011, p.15-17.

<sup>13</sup> M M Lowenthal, *Intelligence: from secrets to policy*, CQ Press, Washington, 2009, p.15-16.

<sup>14</sup> L E Bygrave and J Bing, *Internet Governance: Infrastructure and Institutions*, Oxford University Press, Oxford, 2011, Introduction.

The problems on data collection, mining and processing sharing of ISPs start the controversial arguments at first place<sup>15</sup> but those problems cannot compare with the latest notorious leaks from the former state's contractor, Edward Snowden. The reveals of state surveillance, interception and collection on personal communication and data are highly spotted because US has targeting surveillance on the executive of other states and mass surveillance<sup>16</sup> on everyone in the world. As NSA's PRISM project collect data from the most powerful ISPs Corporations of the world such as Google,<sup>17</sup> Yahoo, Facebook etc. The PRISM project has main objective to watch on every communication devices which connect to the Internet; CPU, Laptop, Pad, Mobile phone. The identification of place time and activity of people could be track and trace orderly from the Big Data Collection<sup>18</sup> that gathering from Everyday-Life practice.

However some states are not in the scope of article since they employ different regime, Russia and China who ignore the democratic value, recognized the threats of espionage via Internet hence they try to construct their own Internet system. The closed system builds up the Firewall, Great Chinese Firewall,<sup>19</sup> which protects the penetration of friends and enemies espionage. Not only External Security reason but also Internal Security reason to control and Surveillance on their people as well.

Nonetheless, the changing strategy form physical weapons proliferation to data collection may relive the concerning on weapon stealing or distributing to the hand of terrorist or rebel groups.<sup>20</sup> But the Collection of data might produce a new threat since the centralized data could bring the secret for missile launching or secret agent profiles of abundant states to central data pool. The risk of leaks or hacks by technicians of terrorist or rebel groups<sup>21</sup> via internet could put the International Security at stake. As the technique for hacking could be accomplished by enormous tactics either physical or virtual attacks, centralized data collection are too risky. The International Regime for managing the risk on personal data processing is required. [I should arrange in the form of – threats to security – risks – problem – centralization of data – create new type of risk by such centralization]

Ever since the end of Cold War, USA initiate the peace process among Super Power by Non-proliferation policy on WMD which create the Hegemony position to USA.(find Quotation and Footnote) However the scandal of secret war on International Internet Espionage harms the peace keeper image and delegitimizes the Hegemony of USA on Global Politics. In the Democratic Society either on Domestic and International level the arbitrary surveillance on personal data is a breach of Human Rights and against the integrity of democracy.<sup>22</sup> Because the collection of personal data is the main tactic and strategy of all Totalitarianism State since Stalin Soviet, Gestapo Nazi and now the NSA of US. The study of different regimes should mention democratic state's regime separately from Totalitarianism because US claims themselves as a Democratic State under Constitution as well as EU & Members are obliged by EUDHR. So the citizen cannot tolerate with illegitimate acts and state must carry out problem with legal framework. Moreover, the concerns on data processing are not only on the sharing of data between ISPs and State but also among States as well.

### Point of Curiosity

- 1) What are the legal regimes of State and International Community on Personal Data Protection? What should be done when those legal regimes confront with dilemma on protecting human rights and using Google's processed data?
- 2) How have the cooperation between state agencies and Google been constructed? How much does it harm the individuals' rights on personal data?
- 3) What should be formulated as a Global governance regime to regulate the data processing of Internet Service providers in order to fulfill Human Rights on Domestic, Regional and International levels?

### Theoretical Framework / Methodology

The article will be undertake within Socio-Legal Study style which will be exploring the Law in action more than Law in a book because the data protection law for ordinary nature are reluctantly cope with situation on internet. Accordingly, the necessity to find out why the personal data violation has happened is related to the relation between state agencies and ISPs. Critical Legal Study would be usefully prescribes the mal-behavior which breach the law and infringe on Human Rights.

<sup>15</sup> M Thompson, 'In search of alterity: on Google, neutrality, and otherness', in *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, T.M.C. Asser Press, Hague, 2012, Introduction.

<sup>16</sup> G Kerschischnig, *Cyberthreats and International Law*, eleven international publishing, Hague, 2013, p. 245-254.

<sup>17</sup> A Lopez-Tarruella, 'Introduction: Google pushing the boundaries of Law', *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, T.M.C. Asser Press, Hague, 2012, Preamble.

<sup>18</sup> M Ingram, Google publishes figures on government requests for data, World Socialist Website, <<http://www.wsws.org/articles/2010/apr2010/goog-a26.shtml>>, accessed on 31/10/2012.

<sup>19</sup> L A Bygrave, T Michaelsen, 'Governors of Internet', in *Internet Governance: Infrastructure and Institutions*, Lee A. Bygrave and Jon Bing (eds), Oxford University Press, Oxford, 2009, Extract.

<sup>20</sup> Y Aubin, and A Idiat, (eds), *Export Control Law and Regulations Handbook: A Practical Guide to Military and Dual-Use Goods trade restriction and compliance*, Kluwer Law International, Netherlands, 2011, p.1-10.

<sup>21</sup> S Brenner, *Cybercrime: criminal threats from cyberspace*. Praeger, California, 2010, p. 121-135.

<sup>22</sup> I Bantekas, (eds), *International Human Rights: Law and Practice*, Cambridge University Press, Cambridge, 2013. Extract.

The chosen case study, Google, could be understood by employing the Post-Structural Analysis which concentrate on the becoming of things in Post-Modernism world especially the act of private corporation in cyberspace. The penetration and operation of Google has been catalyzed by the international economic law which was triggering Globalization and Internet accession throughout the world. Using Giles Deleuze and Felix Guattari Capitalism and Schizophrenia analysis study<sup>23</sup> is enlighten the struggle among multiple actors in cyberspace to shift the 'Line of Flight'.<sup>24</sup> In order to make benefit for their stake, Google even cooperate with others to share and gain more opportunity in this political economy game: Collective behavior; Collusion. The advantage of Google is the high information technology which can connect the data and people in complex connection, 'Rhizome'.<sup>25</sup> These connections and Big Data could be utilized as economic and politic tools to acquire more power in Knowledge-based Society.

The operation of Google and their cooperation with state made a personal data on risk. The more they collected, processed and shared data, the more individual rights were arbitrary breached. In economical law perspective, it brings the consumer rights problems into E-market which could deter customer confident to spend in Cyberspace. In civil and political rights perspective, it harms the democratic legitimacy sphere.

The article on the act of Google can demonstrate the problem on ISPs data processing which may breach the law. For proving the assumption, the evident from their cooperation with state in various perspectives will be scrutinized. However, the prospects to tackle these problems would be extracted from the article as well.

### Regulation Models

With regards to cyberspace regulation, the balance of Individuals freedom and Intervention is relevant to characteristics of specific Regulation Model. Although the Declaration of Independence of Cyberspace propose the independent from state and its legal concepts<sup>26</sup> which governments and corporations mobilized to regulate and control online activities, cyberspace could not legitimately or effectively be governed and needed for legitimacy of regulation by some certain of state sovereigns in combating those harms.

In terms of regulating cyberspace, the legal communities try to provide some alternatives to regulate Cyberspace in 3 prominent alternatives;

#### a) First comes first conquers? Technology Determinism

The first instance of Internet, it is a dominant Technology Determinism<sup>27</sup> which Programmers and ISPs could be a new God in Third Wave Revolution. Our environment and architecture of cyberspace apply a regulatory force, both the law and the wall function as regulatory tools determined by software code. Due to the difficulty of tracking down online perpetrators in different jurisdiction, speech filtering, which can be taken place at the service provider, can occur without users knowing.<sup>28</sup>

Under Google influence, they handle nearly two-thirds of Internet search queries worldwide that most web sites rely on the search engine for half of their traffic. When Google engineers twist its algorithm, they can break the business of a Web site by decreasing their rankings. In this model, states will lessen power over the online, but the government can embed power into the technical architecture of the Internet itself<sup>29</sup> if they want in some "Zone", which will be described in later models.

It seems to be sure that private corporation has a power over information traffic and people will never know whether they share it with government or not.

#### b) Could we just let the Market Driven

USA kept their hand out of the market and allowed regimes in which the widespread use of private speech filtered that made a suspicions about who does the regulating: private entities or the state<sup>30</sup>. Nowadays, the threats to freedom pose by non-state actors, corporations who store huge searchable data.<sup>31</sup> Moreover, they process information, as determined by market. For

<sup>23</sup> G Deleuze and F Guattari, *A Thousand plateaus: Capitalism and Schizophrenia*, trans. and ed. B. Massumi., London: Athlone Press, 1988. (First Published Les Editions de Minuit, 1987.)

<sup>24</sup> Ibid.

<sup>25</sup> Ibid.

<sup>26</sup> J P Barlow, 'A Declaration of the Independence of Cyberspace', 1996, <<http://www.eff.org/~barlow/Declaration-Final.html>>.

<sup>27</sup> L Lessig, *Free Culture: How big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, Penquin, New York, 2004, p.139.

<sup>28</sup> L Lessig, 'What Things Regulate Speech: CDA 2.0 vs. Filtering', *Jurimetrics Journal*, 38, 1998, p. 640.

<sup>29</sup> J Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors', *University of Cincinnati Law Review*, 66, 1997, extracts from pp. 177-205.

<sup>30</sup> L Lessig, 'What Things Regulate Speech: CDA 2.0 vs. Filtering', *Jurimetrics Journal*, 38, 1998, pp. 629-70.

<sup>31</sup> J E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object', *Stanford Law Review*, 52, 2000, pp. 1373-438.

instance, Facebook actually has an economic incentive to make sure that few brands' fans see all advertisers' posts by quietly altering one of its key algorithms,<sup>32</sup> but who are watching it.

With respect to problem of private power, it is noting that the use of online contracts backed by technological protection measures into "Firm Law". However, private power relies on state enforcement of background contract and property regimes, rendering the line between 'public' and 'private'<sup>33</sup> is still on wondering.

c) Creating Cyber Polycentric Regime (Co-Regulation) under People Participation and Social Embeddedness

In addition, the enlargement of search engine and social networks services can pursue a considerable number of new users. Although their personal data will have been processed by private, state authorities might ask for collaboration on specific case.

While online activity offers so much freedom and risk to individual users, which is a paradigm of polycentric regulation<sup>34</sup>, state may increase polycentric regulatory environment by networking government agencies to interact with networked private sector actors, with networked NGOs and other civil society actors actively intervening in process, negotiations and ultimately regulatory activities.<sup>35</sup>

Due to the transcendental nature of cyberspace, the proper model should deprive the idea of nation-state legal jurisdiction and bring in more cosmopolitan approach that seeks to steer a middle ground between territorialism and universalism in which people's multiple community attachments: local, global and non-territorial, and cross-border legal issues<sup>36</sup>

In addition to security technologies, sustaining trust in cyberspace requires rules, transparent practices, accountability standards, and means of redress acceptable to users.<sup>37</sup> Accordingly, International efforts for agreements to protect and sustain cyberspace security are unavoidable in the macro policy.

Howbeit, Netizen might reluctantly accept self-limitation concept and diminish self-interest<sup>38</sup> in order to sustain one's benefits from the commons. Furthermore, the cooperation should extend to control industrial espionage, protect critical information infrastructures<sup>39</sup> or assure information freedom of individual as well.

While cyber-utopianism stipulates what has to be done, Internet-centrism how it should be done<sup>40</sup>. Meanwhile, it is necessary to admit that we, as lawyers, are typically rather poorly equipped to predict the direction technology will take.<sup>41</sup>

However, decentralized network management still needs not only the technologically centralized infrastructures but also democratic regulatory which requires administrative power implementation on rule of law principle.<sup>42</sup> Since, cyberspace not as a place of freedom but as one increasingly of control, online world is one where freedom is curtailed, resembling a series of connected appliances with specifically delimited functionality.

In terms of Cautions, Internet Governance should be managed on the basis of market system self-adjustment, freedom of individual to create innovations, transparency, maximizing limited available resource and complexity sensitive mechanisms.<sup>43</sup>

## Conclusion

To Summarize, It tends to be obvious in numerous cases that state authorities or private sectors having been tagging in cyberspace through various strategies and tactics both officially and even confidentially/unauthorized. However, there is no perfect model for regulating cyberspace to apply with both purposes of protecting Individual Freedom and defending them from Harms as we have discussed above, there are some essential procedures to construct the acceptable regulations for specific communities and interests. In fact, the participation and engagement of people on Cyberspace Regulation tends to be a key point

<sup>32</sup> J Edwards, Facebook Accused Of Changing A Key Algorithm To Hurt Advertisers , businessinsider, 3/10/2012, Accessed on 20/11/2012, <<http://www.businessinsider.com/facebook-changed-edgerank-algorithm-to-hurt-advertisers-2012-10#ixzz2CmzRLVnU>> .

<sup>33</sup> M J Radin, 'Regulation by Contract, Regulation by Machine', *Journal of Institutional and Theoretical Economics*, 160, 2004, pp. 142–56.

<sup>34</sup> J Black, Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes, in *Regulation and Governance*, 2, 2, 2008, pp.137-164.

<sup>35</sup> C Marsden, *Internet Co-Regulation: Internet co-regulation: European law, regulatory governance and legitimacy in cyberspace* , Cambridge University Press, Cambridge, 2011, p. 221.

<sup>36</sup> P S Berman, 'Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era', *University of Pennsylvania Law Review*, 153, 2005, extracts from pp. 1819–82.

<sup>37</sup> Ibid., p.26.

<sup>38</sup> Ibid., p.41.

<sup>39</sup> Ibid., p.42.

<sup>40</sup> E Morozov, *The Net Delusion: The dark side of internet freedom*, Public Affairs, New York, 2011, p. xvi.

<sup>41</sup> D Svantesson, 'A legal method for solving issues of Internet regulation' in *International Journal of Law and Information Technology*, 19, 3, Oxford University Press, 2011, p.262.

<sup>42</sup> T Ogura, 'Electronic government and surveillance-oriented society', in *Theorizing Surveillance: The Panopticon and beyond*, David Lyon (eds), Willan Publishing, Devon, 2006, p.286.

<sup>43</sup> L B Solum, 'Models of Internet governance', in *Internet Governance: Infrastructure and Institutions*, Lee A. Bygrave and Jon Bing (eds), Oxford University Press, Oxford, 2009, p. 86-87.

in Democratic Society. As a campaign of Civil Society and other Stakeholders, there are some solutions to be discussed and brought a concrete policy on Cyberspace such as People participation to check and balance the Authority, Social Embeddedness<sup>44</sup> on Economic activities, Inclusive Netizen-Society and Cultural Diversity.

## References

- Aubin, Y. and Idiart, A. (eds) (2011). *Export Control Law and Regulations Handbook: A Practical Guide to Military and Dual-Use Goods trade restriction and compliance*, Kluwer Law International, Netherlands
- Bantekas, I. (eds) (2013). *International Human Rights: Law and Practice*, Cambridge University Press, Cambridge, 2013.
- Barlow, J. P., (1996) 'A Declaration of the Independence of Cyberspace', <<http://www.eff.org/~barlow/Declaration-Final.html>>.
- Berman, P. S., (2005). 'Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era', *University of Pennsylvania Law Review*, 153, 2005.
- Black, J., (2008). Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes, in *Regulation and Governance*, 2, 2,
- Boyle, J., (1997). 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors', *University of Cincinnati Law Review*, 66
- Brenner, S., (2010). *Cybercrime: criminal threats from cyberspace*. Praeger, California.
- Bygrave, L. A. and Michaelsen, T., (2009). 'Governors of Internet', in *Internet Governance: Infrastructure and Institutions*, Lee A. Bygrave and Jon Bing (eds), Oxford University Press, Oxford.
- Bygrave, L. E. and Bing, J., (2011). *Internet Governance: Infrastructure and Institutions*, Oxford University Press, Oxford.
- Cohen, J. E., (2000). 'Examined Lives: Informational Privacy and the Subject as Object', GEORGETOWN LAW The Scholarly Commons.
- Deleuze, G. and Guattari, F., (1988). *A Thousand plateaus: Capitalism and Schizophrenia*, trans. and ed. B. Massumi., London: Athlone Press. (First Published Les Editions de Minuit, 1987.)
- Edwards, J., Facebook Accused Of Changing A Key Algorithm To Hurt Advertisers , *businessinsider*, 3/10/2012, Accessed on 20/11/2012, <<http://www.businessinsider.com/facebook-changed-edgerank-algorithm-to-hurt-advertisers-2012-10#ixzz2CmzRLVnU>>.
- Google, (2001). Google Motto in internal corporate meeting 2001 on the theme "What Google was all about".
- Ingram, M., (2010). Google publishes figures on government requests for data, *World Socialist Website*, <<http://www.wsws.org/articles/2010/apr2010/goog-a26.shtml>>, accessed on 31/10/2012.
- Kerschischnig, G., (2013). *Cyberthreats and International Law*, eleven international publishing, Hague.
- Kettemann, M. C., (2013). *The Future of Individuals in International Law: Lessons from International Internet Law*, eleven international publishing, Hague.
- Lessig, L., (2004). *Free Culture: How big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, Penquin, New York, p.139.
- Lessig, L., (1998). 'What Things Regulate Speech: CDA 2.0 vs. Filtering', *Jurimetrics Journal*, 38, 1998.
- Lowenthal, M. M., (2009). *Intelligence: from secrets to policy*, CQ Press, Washington.
- Lopez-Tarruella, A., (2012). 'Introduction: Google pushing the boundaries of Law', *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, T.M.C. Asser Press, Hague, 2012.
- Marsden, C., (2011). *Internet Co-Regulation: Internet co-regulation: European law, regulatory governance and legitimacy in cyberspace* , Cambridge University Press, Cambridge.
- Morozov, E., (2011). *The Net Delusion: The dark side of internet freedom*, Public Affairs, New York.
- Ogura, T., (2006). 'Electronic government and surveillance-oriented society', in *Theorizing Surveillance: The Panopticon and beyond*, David Lyon (eds), Willan Publishing.
- Polanyi, C., (2001). *The Great Transformation: The political and economic origins of our time*, Beacon Press, Boston, 2001.
- Radin, M. J., (2004). 'Regulation by Contract, Regulation by Machine', *Journal of Institutional and Theoretical Economics*, 160.
- Siva, V. T., (2011). *THE GOOGLIZATION OF EVERYTHING : (AND WHY WE SHOULD WORRY)*, University of California Press, Berkeley.
- Solum, L. B., (2009). 'Models of Internet governance', in *Internet Governance: Infrastructure and Institutions*, Lee A. Bygrave and Jon Bing (eds), Oxford University Press, Oxford.
- Strasbourg Convention (1981).
- Svantesson, D., (2011). 'A legal method for solving issues of Internet regulation' in *International Journal of Law and Information Technology*, 19, 3, Oxford University Press.
- Towey, R., (2012). 'Internet contribution to UK economy down to e-commerce', <<http://www.peer1hosting.co.uk/industry-news/internet-contribution-uk-economy-down-e-commerce>>, accessed on 1 November 2012.
- Thompson, M., (2012). 'In search of alterity: on Google, neutrality, and otherness', in *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, T.M.C. Asser Press, Hague.
- \_\_\_\_\_, \_\_\_\_\_, <<http://www.google.com/transparencyreport/userdatarequests/faq/>> , accessed on 31 October 2012.

<sup>44</sup> C Polanyi, *The Great Transformation: The political and economic origins of our time*, Beacon Press, Boston, 2001. p.71 and extracts from entire chapter 6.