THE FUTURE OF THE OPEN INTERNET: CHANGING DYNAMICS BETWEEN THE STATE AND PRIVATE INTERMEDIARIES AND THEIR IMPACT ON THE PUBLIC

By

Elena Vladimirova

Submitted to
Central European University
Department of Political Science

In partial fulfillment of the requirements for the degree of Master of Arts in Political Science

Supervisor: Professor Kate Coyer

CEU eTD Collection

Budapest, Hungary
2012

To Mom and Dad

CEU eTD Collection

Abstract

In the absence of adequate state and international regulation of online privacy the future of the open Internet remains in flux. Current framework of notice-and-consent puts the responsibility for privacy protection on Internet service users with minimal requirements to the intermediaries. Notifying users of possible tools to adjust privacy settings on social networking platforms addresses only one aspect of the issue – protecting information from other users. In the meantime, legislators do not address the regulation of relations between the intermediaries and users. For now, internet services are offered on the basis of self-regulation. This means that vast amounts of personal data that are used for commercial purposes are protected neither by the state nor by any international regulatory body. Disruption in the information flows on the Internet has caused growing alienation between the state and the public, which can be seen in migration of the public sphere online. Practices of Internet filtering and surveillance might signal that governments are facing the need to control what information its constituency seeks access to. Since filleting and surveillance in many cases are implemented without notifying the users, these practices show the growing mistrust between the state and the public. Thus, transformation of the role of the public sphere in the process of decision making needs to be addressed on the national level by adopting a comprehensive framework that will enable decision makers to protect personal information online and regain public trust.

CEU eTD Collection

Acknowledgements

I would like to thank my supervisor Kate Coyer for her encouragement and positive attitude when discussing and commenting on previous versions of this thesis. I am also grateful to Lina Dencik for her support and useful suggestions on the literature throughout the academic year. My thank you goes to Eszter Timar for her concern and patience when reading some mess. And finally, to my friends who supported and inspired me in my endeavors, particularly to Betty, Andrey and Katherine.

CEU eTD Collection

Table of Contents

CEU eTD Collection

LIST OF FIGURES AND TABLES

CEU eTD Collection

LIST OF ABBREVIATIONS

ACTA – Anti-Counterfeiting Trade Agreement

DMCA – Digital Millennium Copyright Act

DNS – Domain Name System

GMP – Global Media Policy

IP – Internet Protocol

OSCE – Organization for Security and Cooperation in Europe

PIPA (Protect IP Act) – Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act

SOPA – Stop Online Piracy Act

URL – Uniform Resource Locator

VoIP – Voice over IP

WSIS – World Summit on the Information Society

CEU eTD Collection

Introduction

Year 2011 was important for the future of the Internet users and researchers. Not only was it marked by the events of the Arab Spring, but it also was significant for the human rights activists and international human rights advocacy groups when millions protested against the ratification of ACTA in the EU, and against PIPA and SOPA, two bills proposed by the US Congress. However, the future of the Internet remains in flux. What is at stake is the degree to which there should be regulation to protect users and individual rights, the changing role of the corporations as intermediaries, and the extent to which the state should intervene to protect individual rights and encourage innovation.

The growing concern over the commodification of personal information puts the question of the regulation of the information flows to the forefront of the discussion of globalizing media and communications. In this context, this thesis is concerned firstly with the question of how the information flows should be regulated in the online environment and how this regulation fits into the perspective of free and open Internet. Separate chapters will be dedicated to narrower questions: 1) How the Internet activity is regulated today and whether this regulation is effective; 2) What the changing dynamics of the state-public relations are and what implications they have for the public opinion dissemination and civic engagement; and 3) How the privacy issue is addressed by states and corporate intermediaries.

The relevance of the research to the sensitive issue of privacy online is circumscribed by the process of integration of the online practices with social practices. However due to the fact that online privacy is in practice addressed to a large extent only by private corporations, Internet users can not be sure that what they perceive as private space is indeed a private space. The boundaries between public and private are much more blurred now than ever

CEU eTD Collection

before. With users' concerns over the commercial use of personal information that is gathered in a seemingly private and intimate environment provided by social networking platforms, the issue of the proper regulation of personal information flows in the mediated environment is even more evident.

Public discourse on the topic of Internet regulation is closely connected to the notion of globalizing media and growing complexity of the interactions mediated by it. In general the field of global media and communications is enormous in its recognized multiplicity and heterogeneity. What differs the information flows in the Internet-mediated environment from older media is that it is perceived as extremely difficult to regulate due to its space-less nature. Therefore, there is a lack of understanding of the nature of this particular space and how to approach it.

In this context there is little disagreement on the matter of the Internet surveillance (state or commercial) from an individual's point of view: it is largely perceived as violating privacy, and in a broader context – human rights. At the same time, state authorities defend surveillance policies as providing better homeland security, especially in the light of international terrorist threat, economic crisis, and regime destabilization. The question of balancing security and Internet freedom becomes even more vexing. So far there is no consensus whether we should accept or reject state surveillance in any form, especially in view of the possibility of escalating surveillance practices if positive state regulation is enforced.

CEU eTD Collection

Acknowledging the fact that the issue of surveillance is diverse, I will analyze one of the practices employed by the states – Internet filtering. Internet filtering is distinguished from surveillance by its active interference in the process of Internet browsing, that is blocking certain web sites or separate pages based on its content, whereas Internet surveillance would be less detectable and aimed at recording regular user's activity online without interference, but with the purpose of further in-depth investigation of potentially criminal or risky activities.

In addition to the development of communication technology there is a constant change and transformation of the public sphere due to its integration into the cyber world. In fact a considerable number of scholars see the empowerment potential in the Internet environment. However, I take a more skeptical stance on the issue. On the one hand, the Internet is facilitating numerous processes of everyday life, but on the other, it has caused a shift in the pattern of communication between the state and the public sphere. This change signals more online civic engagement but the lack of offline activism.

The new approach is offered in this thesis to emphasize the importance of the issue and to outline an effective method to address the regulation of information flows over the Internet. An embedded framework of critical and contextual approaches offers to treat online activity in the context of the functions that users perform. Since there are counterparts of nearly any online activity in an offline world, Internet regulation should be drawn from specific traditional spheres. As of now, despite the emerging and evolving global civil society (online social movements, activists, digital rights advocacy groups), state regulation of online activity remains largely informal and nontransparent, even in the old democracies such as the US and EU member-states.

The first chapter of the thesis will provide a general overview of the concepts and approaches to Internet regulation that exist in the literature. I will analyze new regulatory legislature and its implications for intermediary liability and present a new approach to Internet privacy regulation. Chapter 2 will examine the changing dynamics of relations between the state and the public sphere and elaborate on the patterns of decline of the public sphere due to the shift in the Internet-mediated social environment where new intermediaries like social networks enable virtual activism, but to a large extent inhibit off-line action.

CEU eTD Collection

In Chapter 3 the reactions of both states and private corporations to the growing diversity of practices that take place on the Internet are analyzed in two distinct contexts: state Internet filtering practices and their implications for the civic engagement and the issues of privacy in social networks. Put in a broader perspective of the Internet regulation, I will argue that the issue of protection of personal information gathered and processed by private corporations should be of major importance for policy makers.

CEU eTD Collection

CHAPTER I

INTERNATIONAL AND STATE REGULATION OF ONLINE COMMUNICAION

1.1. Concepts and approaches to Internet regulation

In addressing the problem of Internet regulation, different approaches have been offered by scholars. One of the most comprehensive approaches, proposed by Raboy and Padovani (2010), suggests that we need more transparent practices not only on the Internet itself, but in mapping Global Media Policy (GMP) in the first place. The authors recognize the shift from formal and centralized regulation processes to informal. Thought they do not emphasize how this shift affects regulation of Internet and Internet-mediated information flow in particular, the emergence of self- and co-regulatory mechanisms, they state, "have come to be analyzed as networked forms of governance." (2010, 5) As the networked governance implies that decision-making process involves a wide range of public and private actors, we should look at the already existing formal and informal regulatory arrangements for media and communication, including "latent and often invisible processes through which decision-making is informed, such as lobbying, advocacy, interpersonal exchanges amongst policy-makers and media corporate interests." (Raboy & Padovani 2010, 14) Different actors, both governmental and non-governmental, contribute different understandings and knowledge to the process of media policy shaping. Along with the multiple understandings that should be considered, there are also claims for more transparency that come along with them.

However, better understanding of the Internet regulation strategies cannot be achieved through greater transparency of policy-making processes. Some of the attempts to Internet regulation failed because of the perceived complexity of the issue. Instead of referring to the "global interplay among the different "spaces – ethnoscapes, finanscapes, ideoscapes, mediascapes and technoscapes" (Appadurai 1996) or the "growing trans-planetary social

CEU eTD Collection

interconnectedness" (Schilte 2005), we should look for patterns of familiar practices that have been regulated for decades, for instance contractual laws or laws securing the information gathered by banks. Raboy and Padovani support the media complexity approach, suggesting that the uses of communication and the Internet in particular "are no longer served by separately identifiable industries." (2010, 11)

A new approach, which I will employ in this research, is proposed by Helen Nissenbaum (2011) in which the usual calls for more transparency have been abandoned and a very different perspective to treat Internet activity as the continuation of offline social practices is put forward to address the concern with commercialization of personal information. Nissenbaum's analysis of existing practices of privacy regulation concludes that, "there is considerable agreement that transparency-and-choice has failed" (2011, 35) because:

> Concerns over the use of personal information for commercial purposes voiced by privacy advocates, popular media, and individuals have become louder and more insistent in pointing out and protesting rampant practices of surreptitious as well as flagrant data gathering, dissemination, aggregation, analysis, and profiling; even industry incumbents and traditionally pro-business government regulators admit that existing regimes have not done enough to curb undesirable practices, such as the monitoring and tracking associated with behavioral advertising and predatory harvesting of information posted on social networking sites. (2011, 35)

In this context, the role of social networks as intermediaries in the process of dissemination and consumption of information is rapidly increasing, causing transformation of the public sphere. Migration of the public opinion to the online environment, contributes to the alienation between the state and the public, therefore, the once powerful Habermasian public sphere does not exist anymore. Following the rhetoric of Jurgen Habermas and Manuel Castells, failed communication between the state, citizens and civil society, results in the crisis of legitimacy, "because citizens do not recognize themselves in the institutions of society." (Castells 2008, 80)

CEU eTD Collection

Another trend in analyzing the changing environment in which communication from the public to the state flows, is that now with unrestricted and uncontrolled access to information-dissemination technology more actors emerge and compete for the audiences, therefore causing a shift in power relations between the states, civil society actors and corporations. According to Monroe E. Price, this happens along the functions of the "market for loyalties"

> in which large-scale competitors for power, in a shuffle for allegiances, often use the regulation of communications to organize a cartel of imagery and identity among themselves… [these] purveyors of loyalties, including the civil society and interest groups, as well as companies, seek to reinforce the rising tide of commercialization and consumption." (2007, 46-47)

The usual assumption of the market that has to provide competition – and through it more choice – has failed in relation to the Internet policies. The main problem with the absence of adequate regulation of online activity and therefore solid protection of privacy is that in fact there can be no law enforcement implemented to protect even those practices that are outlined in the privacy policies. Self-regulation norms on which all major social services build their privacy policies on is not a law, therefore personal data protection is a user's responsibility. The only one piece of international legislature that is being referred to in the privacy policies of Facebook, Google, and Twitter is the Safe Harbor Framework, which carries an essentially symbolic meaning:

> An organization's self-certification to the safe harbor list, and its appearance on this list pursuant to the self certification, constitute a representation to the Department of Commerce and the public that it adheres to a privacy policy that meets the safe harbor framework… In maintaining the list, the Department of Commerce does not assess and makes no representations to the adequacy of any organization's privacy policy or its adherence to that policy.

CEU eTD Collection

The evidence of the failures to address questions of privacy protection using the notice-and-consent approach, which is certified under the Safe Harbor Framework, lies in the mechanism and framing of choice options. There are only two options that users have to choose between: either agreeing with sharing the information for whatever purposes or not using the service at all. From the perspective of the liberal free market, there should definitely be more options that are problematic to shape given the circumstances of the informational price that has to be paid. Another option, examined by Nissenbaum is to make privacy policies more transparent and user-friendly. However, the practices of Internet users show that most of the policies are long, written in a technical language that is unclear and confusing. For instance, if a user is joining a social network for entertainment and communication purposes, he or she would not necessarily be concerned with privacy protection issues. Elaborating on this option, a decision-making moment might be redefined, that is timely notification can be provided at the point when a user is requested to make a choice whether he or she is willing to proceed and pay the informational price. The calls for more transparency imply that all the practices and steps of gathering information should be clarified for the users. This inevitably makes privacy policies longer and more complicated than they are now. However framed, these options do not improve choice, since the either-or framework remains untouched.

The problem of regulation of the privacy policies lies not only in the outcomes of the notice-and-consent approach. The most notable contradiction of this approach is that it is enacted through self-regulation. Whereas the state-intermediary relations are regulated through the legislature of commercial activities, the intermediary-public relations are not subject to any official policies. I will return to this issue in greater detail further in Chapter 3 when analyzing particular privacy policies of Google, Facebook and Twitter.

CEU eTD Collection

1.2. PIPA, SOPA and ACTA provisions for the intermediary liability

The issue of securitization and Internet governance started gaining its momentum largely due to the potential threat of global terrorism perceived by the governments of such states as the US and the members of the EU. (Deibert & Rohozinski 2010) Several bills, with provisions for such areas of regulation as the copyright law, legal procedures for information disclosure imposed by the state on the Internet service providers among others, originated in the US and EU which pose more questions than they try to address and trigger concerns from the civil society, cyber activists, web site owners and ordinary users. Currently proposed legislature does not meet the requirements not only in terms of regulation itself, but from the perspective of openness to public debate which could foster its efficiency in addressing socially important issues. One of the main points that the legislation seeks to address is copyright protection.

Understandable efforts to protect copyrighted intellectual property, reasonable from the points of view of legislators and content producers and intellectual property owners have serious implications for intermediaries who provide access to these types of content online. SOPA (Stop Online Piracy Act) and PIPA (or Protect IP Act – Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act), both bills proposed by the US Congress House of Representatives in 2011, are intended to impose liability for the content that they provide access to on the intermediaries, such as Internet service providers, which goes in contradiction with the currently enforced public law 105-304-Oct. 28, 1998, named “Digital Millennium Copyright Act” (DMCA) that limited the intermediary liability in 1998. The regulation states the following:

> A service provider shall not be liable for monetary relief, or, except as provided in subsection, for injunctive or other equitable relief, for infringement of copyright by reason of the provider’s transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections. (Digital Millennium Copyright Act 1998, sec. 202)

CEU eTD Collection

Both SOPA and PIPA provide for the court to issue orders in the absence of the owner of the website deemed as engaging in copyright infringing activity and “once the court issues an order, it could be served on financial transaction providers, Internet advertising services, Internet service providers, and information location tools to require them to stop financial transactions with the rogue site and remove links to it." (PROTECT IP Act of 2011, S. 968, § 3(d)(2)).[1] Though the concern of the legislators can be understood as protecting particular interest groups, like media content producers, the bill lacks a clear definition of "infringing activities" that are to be prosecuted.

From the perspective of human rights infringement, both acts – PIPA and SOPA – are claimed to violate freedom of speech and expression and hinder creativity and innovation. (see, for instance, Ammori 2011). Other human rights scholars voice similar concerns. A wave of protest that erupted in January 2012, made the congressmen postpone the further hearings of the bill. When a similar legislation was underway in the European Court of Justice, the ruling in the end of 2011 resolved that "E.U. law precludes the imposition of an injunction by a national court which requires an Internet service provider to install a filtering system with a view to preventing the illegal downloading of files" (CNet News, 2011)

In a similar tone The Anti-Counterfeiting Trade Agreement (ACTA) is aimed at regulating intellectual rights in a number of areas such as pharmaceutical drugs production and distribution, counterfeit goods and media content protected by copyright law. Despite public concerns in the EU, the act was signed by more than 30 states including 22 EU members and the US. The act is currently not in force since no country has ratified it.

International non-profit advocacy groups like Electronic Frontier Foundation, Privacy International and European Digital Rights raised their concern as soon as the negotiation started in 2008. They have pointed out that ACTA not only infringes freedom of expression, but involves violations of privacy that enable surveillance practices sanctioned by the states, adding that none of the non-state human rights or cyber experts was present during its

CEU eTD Collection

[1] In the latest text of the bill (accessed May 25, 2012), the clauses concerning the Internet service providers are removed.

drafting. The European Commission responded to these allegations in the November 2008 factsheet as follows:

> It is alleged that the negotiations are undertaken under a veil of secrecy. This is not correct. For reasons of efficiency, it is only natural that intergovernmental negotiations dealing with issues that have an economic impact, do not take place in public and that negotiators are bound by a certain level of discretion. (2008, 4)

The analysis of the incentives of the states to engage in policy regulations of socially important issues that might potentially imply violations of human rights in the atmosphere of a limited circle of participants, suggests at least three considerations. The first set of incentives might be dictated by the conditions of economic crisis. At the point when other resources have expired, one possible avenue for cash flow might be through the state regulation of intellectual property. Illegal transmission of copyright materials over the Internet, however, should be measured against the implementation costs of the provisions outlined in the acts discussed above.

The second consideration originates from the implicit anti-terrorist agenda. Though the legislators do not acknowledge the potential use of the laws-to-be for surveillance and Internet filtering practices, these acts will enable the authorities to perform unrestricted censoring of the Internet activity. The third consideration is even less explicit, but viewed in a broader context of the changes in the interaction between the state and the public, can offer plausible insights on the purposes of Internet regulation. The unwillingness of the states to address the issues of intellectual property and Internet regulation in particular collectively (as in collaboration with NGOs and various advocacy groups) suggests that due to the emergence of intermediaries in the form of Internet service providers, social practices are affected by the actions of the state to a lesser extent as they used to be and vice versa. The weakening of both the public sphere and the state authority and their growing disconnectedness, which are discussed in the following chapter, contributes to the mutual mistrust and reluctance to seek

CEU eTD Collection

cooperation. Due to the globalization of political issues, to a large extent facilitated by the Internet technology, “we engage in politics without a strong sense of collective social power [and] see power as alien and threatening to us.” (Chandler 2009, 543)

In the context of growing alienation between the state and the public, intermediaries become crucial players, whose powers are currently regulated exclusively on the basis of the legal framework of national or international commerce, in this case offering Internet services worldwide. However, the legislators do not address the regulation of relations between the intermediaries and the public. For now, internet services such as social networking are offered on the basis of self-regulation. This means that vast amounts of personal data that are used for profit-generating commercial purposes are protected neither by the state nor by any international regulatory body. At the same time, privacy issues that are impossible to address through self-regulatory privacy policies are equally important for the Internet users and for the states, as they, among other functions, “play a crucial role in sustaining social institutions.” (Nissenbaum 2011, 44) Strict adherence to legal regulation of privacy would demonstrate respect for human rights and personal information integrity.

1.3. Methodology. Integrated approach to regulation of personal information flows on the Internet

One of the greatest misconceptions of the Internet is that some scholars and policy makers perceive it as extra-territorial, meaning that this environment is essentially devoid of the notion of physical space (see, for instance, Mueller 2010; Herrera 2005; Kobrin 2002) and therefore it remains highly problematic even to attempt its regulation along the same lines as other types of media or social activities such as medical treatment or banking procedures. The seeming placeless-ness of cyberspace has so far prevented policy makers to address the question of online privacy regulation in the conclusive manner. At the same time some prominent scholars admit that online practices are not unique: Held suggests that in fact the

CEU eTD Collection

activities that we currently perform online, i.e. in a global context, are only the amplified reflection of regular social practices (Held et al. 2000, 2). In a similar vein, consider McLuhan's definition of communication technology as "an extension of a man". (1964) However, the present research is aimed at clarifying online practices according to their functional contexts and proposes to take a simpler and clear view of the issue.

This qualitative study seeks to put into the common context the previous efforts to address the issue of online privacy and includes critical analysis of existing legislation as well as comparative analysis of three of the major social networking services – Facebook, Google and Twitter as case studies. In order to provide a common conceptual framing I apply contextual approach to regulation of online privacy. In essence, the author of the approach Helen Nissenbaum claims that nearly all the activities that take place in cyberspace have counterparts in the off-line world.

Contextual approach "takes into consideration the formative ideals of the Internet as a public good" (Nissenbaum 2011, 33), which puts the issue in the nation-state legislative context. The author, however, acknowledges the difficulties related to the regulation of privacy: one of these difficulties arises because of the commercialization of personal information: "In a flourishing online ecology, where individuals, communities, institutions, and corporations generate content, experiences, interactions, and services, the supreme currency is information, including information about people. (2011, 33)

The theory of contextual integrity, contrary to the notice-and-consent – the only required framework that the state suggest intermediaries should apply when designing their privacy policies[2], builds on the offline practices and seeks to view social action taking place on the Internet as parallel to the traditional and legally regulated: "[the approach]

CEU eTD Collection

[2] Privacy policies of Facebook, Google and Twitter that are analyzed in the final chapter work under conditions of notice-and –consent framework. The main idea is to notify users of usual information-gathering practices and the data is handled further. In order to use a service, users have only one option to agree with data-gathering practices.

acknowledges how online realms are inextricably linked with existing structures of social life. Online activity is deeply integrated into social life in general and is radically heterogeneous in ways that reflect the heterogeneity of offline experience." (Nissenbaum 2011, 37) It is through the technological innovations that this transferring of usual practices to the Internet occurred. In terms of regulating privacy online, the Internet should not be perceived as a distinct environment that ought to be regulated anew, but instead the functional context in which the information flow takes place should act as an appropriate domain for regulation.

Any additional information that is generated in the process of migration of a service into the online context and is unique to the Internet environment, such as IP address, cookies and logs, should be subject to the same body of regulation as other information that refers to the user. Therefore, the information that is generated or transferred through the Internet should be subject to the familiar legal procedures, for example, existing between ministries when officials of one ministry request in a written form the information on a particular person retained in the databases of another ministry with a justification of such request.

Together with the contextual approach I use critical research methodology, through which I analyze the legislation in the section above and approach privacy issues in the concluding chapter. It is appropriate for this research since it can accommodate the constantly changing nature of social interaction; it underlines the dynamic dialogue within and far beyond the easily recognizable scope of state-public sphere relations. These constitute a proper framework for embedding a contextual approach to privacy online.

Adopting a critical framework and a similar approach, World Summit on the Information Society participants have also recognized the need for a "multi-stakeholder policy dialogue" (WSIS Tunis agenda 2005, par 67). Another way of looking at this is the concept of "networked governance" that is relevant to my methods because in a critical perspective actions that shape certain practices are as important as actors:

CEU eTD Collection

> “networked governance” [is] the result of “governing processes that are no longer fully controlled by the government, but subject to negotiations between a wide range of public, semi-public and private actors, whose interactions give rise to a relatively stable pattern of policy-making that constitute a specific (and pluri-centric) form of regulation” (Sorensen & Torfing 2007, 4; quoted in Raboy & Padovani 2010, 13)

The way that decision-makers approach the issues of inclusion is that they call for more transparency when, for example, drawing privacy policies and terms of use of commercial websites and services they provide. The prevailing practice to supposedly increase transparency is the notice-and-consent approach or informed consent mentioned above. The gist of this approach is to inform website visitors and users of online goods and services of respective information-flow practices and to provide a choice either to engage or disengage“. (Nissenbaum 2011, 34) There are two main points for consideration in this approach and why it persists despite its inability to protect privacy: it provides a transparent definition of privacy as a right to control information about oneself and the acknowledgement that the information about an individual that he or she has to “share” is a necessary price for using the services.

One more consideration should be accounted for here. There are flaws within the current unregulated commercialization of the information that are relevant for the discussion from the point of view of morality. The relations between the intermediaries and the public are asymmetrical. Consider social networks for instance. For the most part users join social networking sites for entertainment and communication, whereas the owners of the sites act as information-gatherers, bearing intentions to use this information for profit-generating purposes. Such use as has been outlined above is an attribute of the notice-and-consent approach to the regulation of privacy online enacted through self-regulation. Whereas in the contextual approach framework, personal information would be protected by the state legislature.

CEU eTD Collection

Contextual integrity theory provides necessary transparency and clear structure of the Internet and how it is reasonable to approach its regulation. Therefore the central point of the hypothetical regulation is the information flows that are to be treated as entrenched in the respective policy field based on the purpose of the transaction that is carried out on the Internet.

Moving from the methodology of managing privacy online to another under-regulated issue, I will further emphasize the role of intermediaries that now interfere and disrupt direct dialogue between the state and the public. Transforming patterns of power relations lend themselves to the positivist tradition which pinpoints the trends and intentions of state actors to distance them from the public and through policy manipulation, which in the case of online privacy is absent. However, public sphere can still be strengthened should the governments regulate both their relations with intermediaries and privacy issues that arise between the intermediaries and the public.

CEU eTD Collection

CHAPTER II

CHANGING DYNAMICS OF GOVERNMENTS-CORPORATE INTERMEDIARIES RELATIONS

2.1. Transformation of the public sphere. Changing patterns of civic engagement facilitated by the intermediaries.

In addition to the development of communication technology there is a constant change and transformation of the public sphere due to its integration into the cyber world. Starting from McLuhan, who described the media as "an extension of any sense" (1996, 8), and following the argument of Nissenbaum that online practices are now an integral part of our social life, public sphere along with other practices has also largely migrated to the Internet. According to Jürgen Habermas, the public sphere "[is] a domain of our social life in which such a thing as public opinion can be formed." (1989, 231) It seems that with the emergence of the Internet the access to shaping public opinion should have been broadened. Indeed, it is so. However, my argument is that the role of the public sphere as a forum for a meaningful dialogue between the state and the public is diminishing. As one of the components of the public sphere is the state, and due to the changing patterns of online activities that are only beginning to be addressed in terms of their regulation, it can be argued that the public practices have migrated online, but the state's response to this is diminishing interest in public opinion.

One trend in state-public nexus is the increasing commercialization of information and growing individualism that inhibits public discourse. To a certain extent due to individualism, public sphere is failing to act as an independent intermediary between the citizens and the state (Price 2007, 51) Private matters are perceived to be more important than public ones. For instance, Ingrid Volkmer suggests that the ties between private and public matters and the

CEU eTD Collection

evolution of their interdependence are inherent features of the public sphere, however, this relationship "has reversed itself in the 20th century, when these spheres separated." (Volkmer 2003, 14) One of the main reasons for this separation is the alienation of the members of society due to the rapidly developing information technology, which is currently reinforced by the integration of the Internet into everyday lives. When, for instance, in the 18th century the public had to gather in physically existing public spaces to engage in public discourse that was explicitly directed at decision-makers, a strong sense of community emerged (Habermas 1989, 229). Whereas presently, the Internet enables individuals to voice their opinions in an online space occupied by other individuals rather than policy makers who should act on public opinion. The sense of community has switched from physical and moral perception of sharing ideas with the state as a unity of diverse individuals and their interests, to the community of like-minded people.

Perhaps the most important tendency of the public sphere transformation in the context of this thesis is the increasing role of private intermediaries facilitated by the development and penetration of communications technology into social canvas. This tendency is not specific solely to the Internet as an intermediary, and put in a broader context, again following McLuhan, the reality is that "the living room has become a voting booth." (McLuhan & Fiore 1996, 22). Therefore, the public sphere as a mediating sphere between state and society has been substituted with the Internet environment, the most influential intermediary. Despite a certain success of online public sphere to influence political situation, as it will be discussed in the following section, civil movements and groups that actively function online, face the risk of losing momentum to actually participate in a discussion addressed to policy makers.

An increasing role of the Internet as an intermediary and the role of private corporations in the form of Internet service providers have shifted not only the patterns of public participation in decision-making processes, but also in the flow of information. (See

CEU eTD Collection

figures 1 and 2, identifying the shift) Figure 1 shows traditional triangulation of cooperation between the state, mass media and the public. Bi-directional links suggest that the exchange of opinions and decisions between the actors is reciprocal. In case of communication between the public and the state, public opinion is voiced through NGOs, interest or advocacy groups; the response is transmitted using broadcast corporations and printed press. All the relevant actors are perceived as of equal importance.

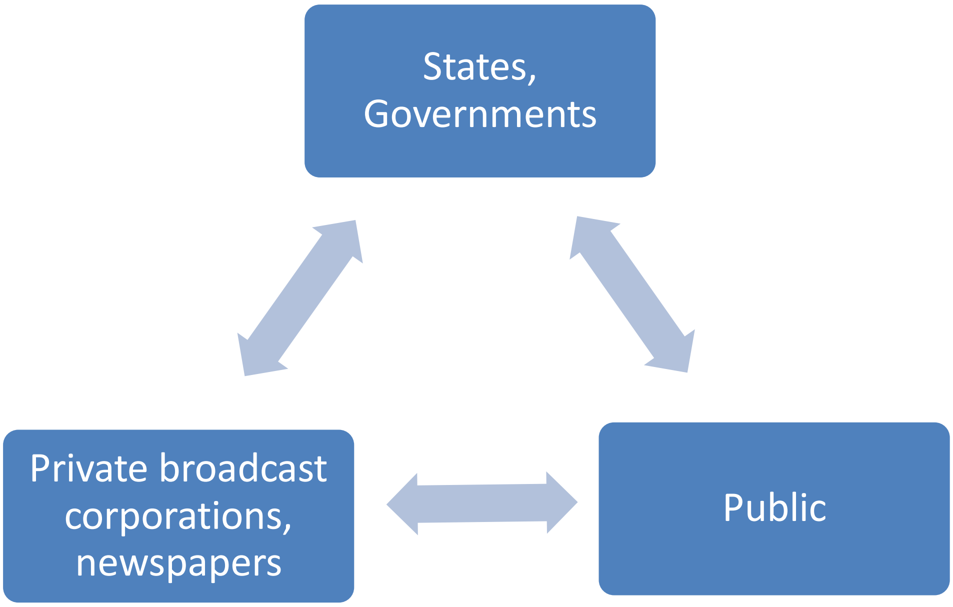

Figure 1

The patterns of interaction between the three groups of actors: the state, the public and traditional private corporations, such as television and newspapers in the public sphere

Figure 2 (see below) demonstrates the shift in the role of private corporations who act as intermediaries, and distortions in information flows caused by their central position in the process of conducting public opinion. These distortions, however, do not cancel direct information flows between the state and the public, but in the presence of Internet service providers, for instance in the context of privacy protection, signify states' weakened ability to cooperate with the public sphere. The actors are perceived as differentiated in their influence.

CEU eTD Collection

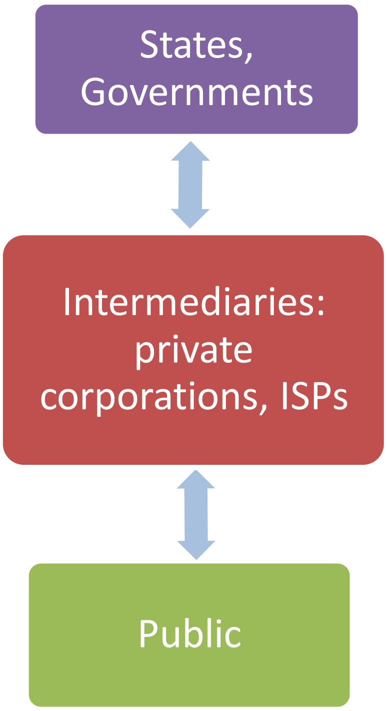

Figure 2

Structural transformation of the public sphere where private corporations have shifted to their intermediary role. The link between the state and society is weakened and intermediaries in the form of the Internet service providers provide the environment for public opinion shaping.

Another way to visualize the shift in public-state interaction is through a linear process of public opinion dissemination in Figure 3.

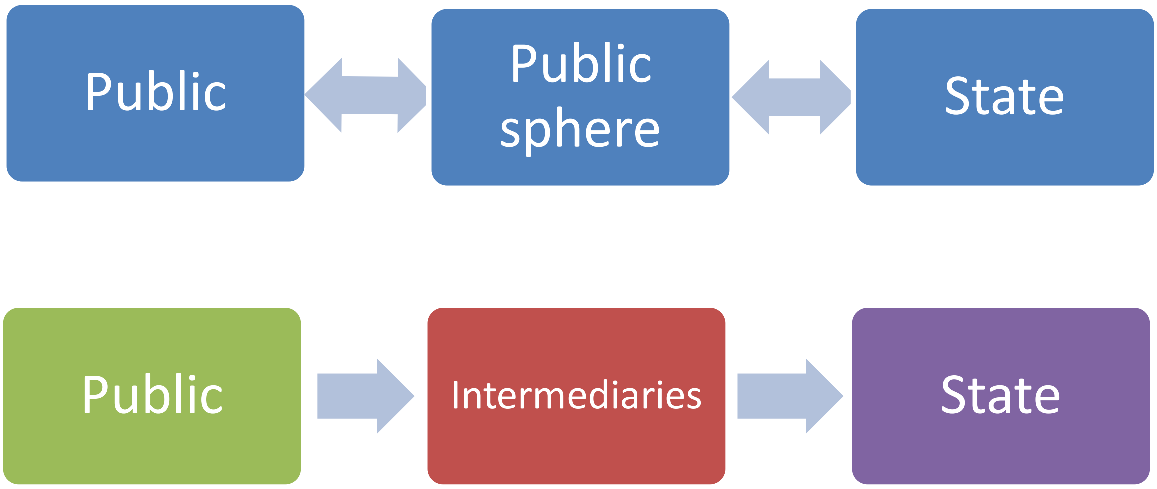

Figure 3

The role of mediator has shifted from the public sphere to intermediaries

CEU eTD Collection

In this transformed structure of information and public opinion flows, public sphere is characterized by a weakening of its critical functions. This also signals the diminishing role of the state as a just and democratic decision-maker. In addition, failure or reluctance to communicate with public directly entails that states are less likely to act on public opinion being articulated on the Internet, which In its turn, leads to neglect and violation of human rights and liberties. The balance that persisted when the media was perceived as the fourth branch of government along with NGOs, interest groups and broader civil society, has been upset by the now more prominent position of private corporations. Some scholars, for instance Price (2007) and Castells (2008), argue that this transformation is preferable for the civil society groups as it eliminates barriers to entry into political cartel and expands the circle of actors:

> [c]ivil society groups … support changes in the infrastructure of communications that permit greater ease of multi-site access. Intermediaries begin to foster and advocate, often under neutral auspices, policy structures that permit global advocates to be more effective in achieving their goals. Obviously, the new sellers favor a multi-channel universe, one that expands the numbers of platforms locally because of altered technologies. (Price 2007, 50)

Meanwhile, there is a danger that instead of one public sphere that is meant to articulate public opinion to policy makers, there emerge multiple public spheres and they therefore represent special interests rather than the whole society. Special interest are crucial in producing information and drawing public attention to certain issues (Lohmann 2003), but at the same time special interest cannot be expected to be relavant to the majority of the public. This indicates how a public sphere that formerly emerged from the structure of society must now be produced circumstantially on case-by-case basis. The central relationship of the public, political parties, and parliament is also affected by this change in function. (Habermas 1989, 236)

Apart from the distortions caused by the pervasive effects of the increasing role of intermediaries, to a certain extent this alienation between states and their constituencies can

CEU eTD Collection

be attributed to the globalizing character of policy-making. In view of global terrorism threat, for instance, and acknowledgment of the fact that this issue cannot be addressed only on the nation-state level, governments seek not public opinion but inter-state support. However, states, being the only legitimate actors on the international arena fail to embrace globalization. This failure refers to the hampering of the development of interconnectedness between the states and pushes them back into regionalism (Stanton 2007, 104).

This slide into regionalism emphasizes the assertive role of governments in the process of policy making. For instance, Chandler (2009) suggests that the reverse is also true, that "the more globalized politics becomes, the more governments are reduced to the role of advocates and activists", therefore shift towards the global can be perceived as a withdrawal from social engagement and political struggle. (2009, 542-44). But this trend should not be attributed only to the shift in states' functions; social movements and activists, due to the strengthening of intermediaries, are also affected. The more their activities are mediated, the less offline action and influence on the government they can produce.

Going back to the issues of miscommunication or lack thereof between the state and the public, it should be noted that it occurs when the civil society does not have incentives to form public opinion. The reasons for the lack of interest in public issues could be individualism and consumerism that I discussed above. However, malfunctioning of the civil society has serious implications for the representative democracy. For example, Castells (2008) and Stanton (2007) agree that without an effective civil society the state is alienated from the public: "[unable to fulfill] the demands of interaction… the whole system of representation and decision making comes to a stalemate. A crisis of legitimacy follows because citizens do not recognize themselves in the institutions of society." (Castells 2008, 80) Inability of the government to relate to the public leads to a crisis of authority. In the past decade, surveys of political attitudes around the world have revealed widespread and growing

CEU eTD Collection

distrust of citizens vis-à-vis political parties, politicians, and the institutions of representative democracy (Castells 2008, 82). In this situation the role and support of NGOs and civil movements increases, therefore undermining the role of governments. However, compared to the resources that are at the disposal of the state, NGOs at large are somehow limited. With the growing alienation between the state and the public there are signs that most of the time civil society does not have a say in policy discussion involving such issues as, for instance, human rights or engaging in military operation as in the case of military intervention of Iraq in 2003 despite public protests against it. Therefore, NGOs and civil movements sometimes perform a symbolic role of public engagement that despite numerous efforts, not affect state policies. The ultimate role of the state as the primary policy maker that is emphasized in the context of Internet regulation can be diminished if the adequate legislation drafted with the active participation of all the relevant actors, including NGOs, advocacy groups and think-tanks. Re-balancing of the actors' positions in the process of policy-making is necessary for producing effective and human rights-friendly Internet policies.

2.2. Social media as a tool for online and offline activism. Empowerment capabilities of the Internet.

The emergence of the Internet as a political tool constitutes a gradual movement, the impacts of which are widely disputed and largely unpredictable. The empowering effects of using Internet technology could not be predicted or foreseen. To a certain extent accidentally, such events as the Twitter revolution in Iran in 2009 and the sequence of the Arab uprisings in the beginning of 2011 and their coverage in the Western media, have drawn the attention of the governments across the world to a set of possibilities and ways of civic engagement and new means of asserting even greater control of their societies in authoritarian regimes and, to the surprise of many, inspired greater interference into privacy in the democratic states.

CEU eTD Collection

Hilary Clinton's optimistic outlook on the empowering capabilities of the Internet, pronounced in 2010, recognizes that "new technologies do not take sides in the struggle for freedom and progress." However, the parallel with the collapse of the Soviet Union by means of samizdat, should be seen as an exaggeration, for the Internet practices of blogging, e-mailing, twitting and the like, lack a very important component, that made those "courageous men and women" international heroes "who made the case against oppression" – their actions, including the process of dissemination of information, took place in an offline world. The difference between the two upheavals is that in the cases of Iran or the Twitter revolution and the Arab spring people were empowered by the intermediary tools that the Internet provided, which, in my opinion, had a significant impact in the beginning of the protests, but exhausted itself due to its mediating position, the lack of mutually binding and long-lasting feeling of community that supports public sphere, as for instance, Evgeny Morozov rightly points out in his book. (2011) This trend of shifting activism and patterns of civic participation was acknowledged as far as in 1964 by Marshall McLuhan, for instance in his reference to the political processes that people engage in without leaving their home (McLuhan & Fiore 1996, 22)

A tendency, apart from the exhaustion of the driving force of community, that encourages and facilitates online participation but inhibits the offline action, is the increasing filtering and surveillance practices employed by the state and carried out by, for instance, social media. This issue will be addressed in more detail in the third chapter. The flourishing Internet technology can both empower and facilitate a civil movement, but at the same time it also enables oppressive regimes to employ intelligence practices. For example, both during the events in Iran in 2009 and in 2011 the same technology – SMS – was used to navigate the movement of protesters, and at the same time, was used by the state authorities to notify citizens about the imminent persecution in case these people take to the streets.

CEU eTD Collection

In sum the argument is that optimistic outlook on the Internet capabilities does not provide a realistic picture of all the potential uses of the Internet and does not acknowledge unlawful practices that can be mediated by it, consider, for example, cyber terrorism and surveillance. Andrew Calabrese sums up the present argument:

> On the one hand, the institutions, technologies and policies that make up what we call "the media" are tools in the aid of cultural commodification, excessive consumption, market censorship, political surveillance and the invasion of privacy. On the other hand, those same tools are means by which actors engaged in struggles for social justice are able to organize, coordinate and mobilize… (2005, 302-303)

In the context of oppressive regimes it is problematic to refer to the issue of alienation between the state and the public, which has been discussed in the previous section, since human rights and public participation are not a priority for the authorities. However, this can be referred to not as a changing dynamics, but the long-lasting reality that we nevertheless have to address. Basically throughout the world, civil societies now have the technological means to exist independently from political institutions and mass media. Some scholars like Volkmer and Castells see an empowering effect of this independence, but I argue that separation of the public from the state alarms that public opinion is either does not reach decision makers or is of no value for them.

Apart from the suggestion that technology empowers public discourse, enabled by the intermediaries, it tends to stay in the online environment rather than pushes decision makers to act on public opinion. It should also be noted, echoing Morozov's argument that the spread of information dissemination technology and the increasing number of access points do not automatically entail active political discussion and civic engagement. In fact, one of the observations that Morozov offers is that "[the Internet] empowers the strong and disempowers the weak" (2011, xvii) finds its illustration throughout the events of 2009 and 2011, when the authorities used the same tools as activists to track particular individuals in order to persecute them. Such Internet services as a social network Facebook played an important role in both

CEU eTD Collection

dissemination of the information about the protests and in helping the authorities to identify the dissidents.

Despite the ambiguous use of the Internet by state officials, some scholars prefer to see only the liberating potential in the Internet environment. (Barber 1999, Rash 1997) The cyber-optimists claim that through the Internet-mediated public sphere human rights activists and civil society pull their actions together and convey and defend their views avoiding the state-related practices. Whereas cyber-skeptics acknowledge the governments’ ability to use the Internet the same way as the older types of media, like newspapers and television – to manipulate public opinion, but what is more apparent nowadays is that due to the fact that there is no effective domestic or international regulation of the Internet on the issue of privacy protection, the governments can use it as a means of coercion and surveillance. With the growing public distrust in the government and alienation, partly reinforced by the emergence of intermediaries, Internet users seek to engage in public discourse using private commercial services such as social networks. However, this seemingly private environment can be used by the state as an access point to alter or intervene into the process of shaping public opinion or to influence political situation. There are instances when state officials contact private intermediaries in order to use their services for political reasons, for example, the US State Department asked Twitter to hold off the site maintenance to prevent service disruptions during the Twitter Revolution in Iran in 2009 (Morozov 2011, 11).

There are frequently encountered references to the manipulation of the Internet services employed by authoritarian regimes; nevertheless, we should admit that democratic governments put the Internet to the same or even more sophisticated use. Analyzing the discussion on the bills and signed laws in the US and EU presented in chapter 1, and the reports made by researchers of human rights organizations and think-tanks such as Privacy International and CitizenLab, it would be biased to conclude that only closed regimes are

CEU eTD Collection

prone to Internet surveillance and violation of human rights. Questions associated with an inadequate use of the Internet by democratic governments, for instance, were discussed at the Conference on Digital Rights Advocacy in Budapest, 2012, where one of the concerns was that nowadays in the absence of proper Internet regulation, especially in the field of protection of privacy, state officials in the US and UK start surveillance procedures without a warrant or any other notice of the reason for doing so. Such Internet services as social networking platforms provide a fruitful context for gathering personal information on the users that the states have no difficulty to obtain. This problem is discussed in greater detail in the final chapter of this thesis.

CEU eTD Collection

CHAPTER III

STATE AND PRIVATE PESPECTIVES ON THE INTERNET REGULATOIN

3.1. Internet filtering: basic concepts, techniques and implications for intermediary liability

The issue of Internet freedom and the leading role of Western democracies in fostering democratization through the Internet, addressed by Hilary Clinton in 2010, raised a new wave of cyber-optimism as well as awareness of the pervasive practices of authoritarian regimes that continuously violate human rights using online technology. However, no concrete and specific suggestions have been made so far to tackle the issue and how to address it. In the meantime, not only oppressive regimes engage in Internet filtering, but democratic states, such as the US and EU member-states press for new laws that will enable the governments to control and direct information flows over the Internet and impose liability on Internet service providers. In the absence of proper all-encompassing regulation of online practices, some states now engage in uncontrolled Internet filtering and surveillance.

In the opening section of the thesis I have already outlined some differences between Internet filtering and surveillance like the absence of interference in the users' online practices in the latter case, one crucial feature should be mentioned here as well – while filtering does not target any particular individual, restricting access to particular online content, Internet surveillance implies that the state has already identified the subject for intelligence and is targeting individual persons. In this context the future of the open Internet remains unoptimistic, however, the practices and the motives of Internet filtering have to be studied in more detail and necessary regulation has to be enforced in order to secure the freedom of expression online.

CEU eTD Collection

Studies of Internet freedom are conducted by research centers and non-profit NGOs like Privacy International (UK) and CitrizenLab (Canada-US) on a regular basis to perform watchdog functions and provide accounts of state and corporate Internet surveillance. In this research I am using the reports of the OpenNet Initiative[3], to provide a realistic, though perhaps an incomplete picture of current Internet practices used by the states to illustrate the impact of unregulated use of the Internet and its implications for regular citizens and civil society activists.

Many countries around the world block or filter Internet content, denying access to information — often about politics, but also relating to sexuality, culture, or religion — that they perceive as offensive or harmful for ordinary citizens. In one of the first encompassing studies of Internet filtering patterns, Robert Faris and Nart Villeneuve rightfully notice that "Claiming control of the Internet has become an essential element in any government strategy to rein in dissent – the twenty-first century parallel to taking over television and radio stations." (2008, 9) The extent of what is deemed dissenting by the authorities varies across countries, but the ever-increasing use of technology to control access to and flows of information is a worrisome signal for the Internet freedom.

Instead of simply acknowledging the fact that Internet filtering takes place, a far more insightful approach should be taken to identify the rationales for this practice. The research has revealed at least three motives for Internet filtering: politics and power, social norms and morals, and security concerns. Though the perceived threat to national security is a common rationale used for blocking content, Internet filtering that targets the web sites of insurgents, extremists, terrorists, and other threats generally garners wide public support. (Faris & Villeneuve 2008, 9) However, these rationales vary across countries and are largely shaped by the social and political context in each individual state. For instance, protection of intellectual

[3] The OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa). http://access.opennet.net/about-the-opennet-initiative/

CEU eTD Collection

property is another important issue of targeted Internet regulation, particularly in Western Europe and North America." (Faris & Villeneuve 2008, 9)

Another dimension across which the discussion of filtering practices revolves is the lack of public knowledge about filtering or even support of such state practices. In traditional societies of Middle East and Asia, as the research shows, users can suggest web sites for blocking, like porn content in Saudi Arabia, or call for increased filtering of certain websites. (Faris & Villeneuve 2008, 12) Though public support for blocking of particular web sites on socially sensitive issues is not surprising, internet filtering on political grounds is usually less popular, with one of the exceptions being that authoritarian states may resort to Western intervention rhetoric. However, regime destabilization as a rationale for interfering practices of the state is increasingly more difficult to justify to the public, especially with the penetration of Western media and entertainment that finds its audience in Oriental countries. Keeping in mind the recent happenings like Twitter revolution in Iran in 2009 and the Arab Spring, allegations of Western interference in sovereign nation-states are becoming less popular in these societies, since it is largely accepted by now that it is not mere Western technology that triggered the uprisings, but the internal political pressures and discontent. (Morozov 2009)

The states that filter the Internet do not restrict themselves to the spheres of public interest, they also engage in protecting corporate interests by, for instance, blocking web sites where people can download communication software. A popular service that enables making phone calls over the Internet has been under attack on numerous occasions. The use of Skype VoIP (Voice over Internet Protocol) technology "reduces the customer base of large telecommunications companies, many of which enjoy entrenched monopoly positions". This service, for instance, has been blocked in Myanmar, United Arab Emirates, Syria and Vietnam. (Faris & Villeneuve 2008, 13)

CEU eTD Collection

Diverse content targeted by blocking requires rather unsophisticated techniques that are incorporated into the usual set of procedures of ISPs. Technical dimensions of Internet filtering can be implemented at two major levels, at the servers of ISPs inside the country and the international gateways:

> ISPs most often respond quickly and effectively to blocking orders from the government or national security and intelligence services. Therefore they block what is requested in the cheapest way using technology already integrated into their normal network environment. Blocking by IP can result in significant overblocking as all other (unrelated) web sites hosted on that server will also be blocked. (ibid.14)

In broader understanding of state surveillance Internet service providers play a crucial role in what we can access online, but only the states have all the necessary resources to make ISPs engage in Internet filtering. One of the means by which state authorities can require intermediaries to comply is through withdrawal of a license under which an ISP provides its services, and considering the fact that there are usually several of them even in the smallest of states, Internet service providers can suffer the same way as users whose experience online is restricted to what the government allows them to access.

Among the most common techniques of internet filtering are IP blocking, DNS (Domain Name System) filtering and URL (Uniform Resource Locator) filtering, being the most accurate one, when only a particular page of a website is blocked. Domain name system, described simply, is a database of all the word-names of websites and their proper IP addresses; when the filtering is implemented in DNS the required domain name will basically be disassociated with its numerical address. (Faris & Villeneuve; Murdoch & Anderson 2008)

Apart from the technical complexities of the issue, there are more important aspects that are of primary concern of this thesis. Technical capabilities of the state can indisputably be immeasurable, but there is a problem of accountability to the public that is at stake here. Though in some occasions states can justify their actions and pacify the public when concerns are voiced, for instance with the reference to terrorist threats. As Stanton correctly points out,

CEU eTD Collection

"public opinion is a powerful thing. It has the capacity to alter or shift the balance of argument and to transform an objective so that it fails or succeeds in opposition to its original goal, [but] it can be easily influenced […] most notably by the threat of global terrorism." (Stanton, 2007, 103) Nevertheless, more pervasive interference in privacy matters goes in direct violation of human rights. Increasing concerns with state surveillance of ordinary citizens, for instance, are now among other issues of monthly discussion in Wired Magazine, seek to draw the attention of policy makers and concerned public to the issue of online privacy and Internet freedom in general. This matter has been prominent in relation to surveillance practices in the US and EU.

Despite the popular belief that Internet brings democracy, related Internet control mechanisms are also in place in Canada, the United States and a cluster of countries in Europe. However, another research conducted by the same research body – OpenNet Initiative in 2010, indicates that in developed democracies Internet filtering is substituted with pervasive surveillance that is even more compelling as it targets particular individuals without any warrant or notice. As Ronald Deibert and Rafal Rohozinski suggest, with more sophisticated tools emerging every year, internet censorship is going beyond a mere denial of service or blocked pages; it is becoming more assertive and normative:

> States no longer fear pariah status by openly declaring their intent to regulate and control cyberspace. The convenient rubric of terrorism, child pornography, and cyber security has contributed to a growing expectation that states should enforce order in cyberspace, including policing unwanted content. Paradoxically, advanced democratic states within the Organization for Security and Cooperation in Europe (OSCE) — including members of the European Union (EU) — are (perhaps unintentionally) leading the way toward the establishment of a global norm around filtering of political content with the introduction of proposals to censor hate speech and militant Islamic content on the Internet… No longer is consideration of state-sanctioned Internet censorship confined to authoritarian regimes or hidden from public view. Internet censorship is becoming a global norm. (Deibert & Rohozinski 2010, 4-5)

Usual justifications and attempts at affirmative regulation do not undermine the impact of surveillance on private lives of the people and have far more serious implications for

CEU eTD Collection

activist communities that increasingly rely on Internet technologies for communicating their actions and carry out their practices. Overall, state interference with the Internet practices suggest that there are political rather than social incentives for asserting control over the Internet. The weakening state authority and mutual mistrust between the state and the public, in part caused by the chaotic and unregulated Internet environment, discussed in chapter 2, is one of the possible explanations of decreasing Internet freedom.

3.2. Private corporations' approach to online privacy regulation. Cases of Facebook, Google, and Twitter.

3.2.1. Trade-offs of using social networks

Apart from the state-led practices that undermine freedoms of speech and expression, there is another equally important area of concern. Private corporations in the Internet-related industry have become powerful intermediaries between the state and the public, and their role is far from being understood and examined substantially. In this chapter, the main focus will be on analyzing privacy policy of Facebook. Google and Twitter fit in the same conceptual framework of notice-and-consent self-regulation practices. The difference between all three intermediaries is circumscribed by the services they provide and scopes of functions that users can perform in each of these platforms.

With the development of internet technology it becomes easier both for state and private actors to penetrate into the lives of individuals. Some of the implications discussed in previous sections suggest that tat apart from reason and justification of such intrusions, there are instances when we routinely sacrifice privacy for convenience and security, or even willingly disclose personal information. Social networks provide a perfect context for sharing ideas and information which is later collected by data-gatherers and used for commercial purposes. Though data collection and retention practices are not new, the use to which

CEU eTD Collection

personal information is put by private intermediaries is a relatively recent phenomena. Creators and managers of the biggest data-gathering corporations – Facebook, Google and Twitter – claim that they did not intend their services to be used for profit-generating purposes (Nissenbaum 2011; Morozov 2011). However, analyzing the amount of information that is being collected, it is only logical to use it as a valuable commodity with the state being one of the primary buyers of this good.

This development cannot be extracted and examined out of the context of media globalization. Adoption of such notions as network society (Castells 1996) mentioned above, can be viewed as an acknowledgement of information and communication technologies as facilitators of democratic governance.

> The relationship between technology and society is that the role of the state, by either stalling, unleashing, or leading technological innovations, is a decisive factor in the overall process, as it expresses and organizes the social and cultural forces that dominate the given time and space. (Castells 1997, 13).

Having discussed the implications of this cyber-optimistic view in previous sections, I have argued that along with the empowering and facilitating powers of social media, there are numerous examples of these tools being used to manipulate public opinion or threaten civil activists. With the growing public distrust in the government, partly due to the emergence of intermediaries, the Internet users seek to escape state control using private commercial services such as social networks. However, reliance on private service providers cannot protect users from state interference. As Morozov reports in his book, state officials of the US State Department asked Twitter to hold off the site maintenance to prevent service disruptions during the Twitter Revolution in Iran in 2009. (Morozov 2011, 12) This seemingly innocent interference suggests that administrative resources can be employed the same way to request personal information stored in the social networks.

With the users who perceive social network environment as intimate and secure on the one hand and ill-defined privacy policies that enable personal data aggregation on the other,

CEU eTD Collection

for some individuals there is a problem not to make one's voice heard, but rather to stay invisible, which is becoming problematic due to the increasing number of instances of state and commercial surveillance, performed via social networks. This feature is not longer available in the context of social networks is of great significance for online activists whose activity might be perceived as threatening political authority. As Craig Calhoun suggests, "globalization has all along included an element of surveillance, which has always been a matter of data management and analysis as much as observation, and which has benefited from technologies to improve each." (Calhoun 2002, 2) For some individuals the matter of surveillance becomes irresolvable, since they might need social media for working purposes or coordinating of certain activities, but they are forced to sacrifice personal information in order to use the services or sometimes not knowing how exactly their information is used. As Nissenbaum argues, the presence of the transparent privacy policy does not protect privacy since it might require time, effort and sometimes expert knowledge and attention to details that are often omitted in privacy policies. (2011, 42)

3.2.2. Surveillance in social networks

These days with the development of internet technology and emergence of social networks, it is unlikely that people would stay out of these networks purely because of the privacy concerns. As will be discussed further in this chapter, the majority of the users are concerned with privacy issues, but due to certain factors they still use social networks. In many ways they not only enable participants to stay in touch with distant friends and acquaintances, but to a large extent social networks, like Facebook, help to facilitate off-line communication.

An ongoing debate among social scientists and ordinary Internet users is focused on the phenomenon of social networks in relation to commodification of personal information

CEU eTD Collection

and privacy. The emergence of social networks in 2004-2005 was a new social phenomenon that took several years for media scholars to categorize and define. boyd and Ellison (2008, 211) define social network sites as

> web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system".

This technical definition accounts for practices that users can perform within the social platforms, but does not present the role of those who run these platforms. First emerging as a free social network in 2004, Facebook with the most user-friendly interface is now a №2 most visited site on the web (alexa.com, accessed on May 25, 2012) following Google on the first place. Multi-billion business whose revenues are generated by selling statistical information on any required sector of the population. Facebook now is the largest database of more than eight hundred million people (current number of active users as of the beginning of 2012) who willingly submit their personal data, but unlike participating in a survey, are not notified how exactly their personal data will be used and are not offered any compensation for sharing it. In its initial from Facebook, according to its founder Mark Zuckeberg, was built "to make the world more open and transparent, which we believe will create greater understanding and connection. Facebook promotes openness and transparency by giving individuals greater power to share and connect". This is still the leading principle of Facebook (Facebook 2012), despite its transformed operational purposes.

One of the prominent authors who is engaged in a discourse about privacy in social networks is danah boyd[4], a senior researcher at Microsoft Research and Harvard. According to boyd, "Privacy is a sense of control over information, the context where sharing takes place, and the audience who can gain access. (boyd 2008, 18) This definition of privacy can

CEU eTD Collection

[4] Spelling is presented as it is given on the authors website http://www.danah.org/ and in other scholarly articles (see Fuchs 2009)

be misleading, for instance Helen Nissenbaum suggests that in the context of social networks, control over personal information is very problematic. Because of the notice-and-consent approach embedded into social network privacy policies, the function of control is limited to opt-in or opt-out possibilities. (Nissenbaum 2011, 34)

Issues of control over personal data are central to the understanding of privacy, since privacy is still a debatable notion. For some users such data as real name, address, cell phone number and relationship status are relatively personal, whereas for others those are pieces of public or general information (boyd and Marwick 2011, 1) therefore, can be easily made visible to any visitor of the Facebook profile.

Starting from 2006 when Facebook introduced NewsFeed, there has been a wave of concern voiced by its users over the fact that basically every interaction or exchange of information they made on-line was visible to everyone on their friends' list, including those to whom they might not be willing to show this particular step (boyd 2008, 13). This feature exists on Facebook today, as a useful tool of keeping track of friends' events. At the same time, the website administrators not only explain, but give guidance to how to adjust privacy settings in the Privacy Policy, in the section "Information we receive and how it is used". (Facebook 2012) [5] At the same time the dualism of the question of privacy is the fact that people like to know private information about others but most of them are not willing to share their private data. This fallacy of human nature is widely used by social networks and as danah boyd claims that "[c]ognitive addiction to social information is great for Facebook because News Feed makes Facebook sticky. But is it good for people?" (boyd 2008, 13) In addition to the author argues that "Facebook users felt exposed and/or invaded by the architectural shifts without having a good way of articulating why the feature made them feel uncomfortable. The reason for this is that privacy is not simply about the state of an inanimate

CEU eTD Collection

[5] The features News Feed and Mini-Feed were introduced with additional privacy controls shortly after users' protests in 2006. Facebook Timeline. September 2006.

object or set of bytes; it is about the sense of vulnerability that an individual experiences when negotiating data. (danah boyd 2008, 14)

From a realistic perspective, a commercial organization such as Facebook cannot be held responsible for the perception of privacy issues or feelings about the implementation of certain practices. However, analyzing the previous arguments through the contextual approach, in case the users feel their right to privacy has been violated, there should be ways to still use the services, but require the intermediaries to take responsibility. Now within the framework of informed consent only users are responsible for protection of their privacy.

3.2.3. Audiences and their perceptions of privacy

As many scholars agree, social networks are generally focused on young people as a target audience (Fuchs 2009, 4). Young people are usually perceived as careless and trusting, which makes them less likely to voice privacy questions and doubts. At the same time they are also more perceptive to new technologies and features on the site, therefore the example of News Feed can be interpreted as when new privacy settings were introduced in September 2006, many Facebook users could adjust their profiles and the information they shared with others in such a way as to ensure it would not be seen by unwelcome users. However, it should be noted that adjustments to privacy settings do not change the information that is available to the intermediaries.

Another distinct feature of social networks that should be taken into account is that joining those is technically voluntary. Users are not forced to join an online social network, and most networks we know about encourage, but do not force users to reveal - for instance - their dates of birth, their cell phone numbers, or where they currently live. “And yet, one cannot help but marvel at the nature, amount, and detail of the personal information some users provide, and ponder how informed this information sharing is. (Acquisti and Gross 2006, 1).

CEU eTD Collection

Not only joining the networks is voluntarily, but also the amount of information that one shares is as well decided individually. But the way the network structure encourages users to share more information can be recognized as psychological pressure or in sociological terms “framing”, “nudging” or constructing “choice architecture”. (Thaler and Sunstein 2008). By sharing more information users want to find more “friends” who share common interests. With the recent tendency to substitute real live interaction with virtual one, this urge to reveal private information can be attributed to the fact that in the case of Facebook, half of its eight hundred million users log in to the site every day and on average, more than 250 million photos are uploaded per day. (Facebook Statistics 2012)

Various studies and surveys were conducted to provide a better understanding of perception of privacy issues by both social network users, who mainly consist of young people and their parents. The majority of scholars admit that perceptions of privacy are correlated with the age of users. Acquisti and Gross’s research on privacy attitudes shows that:

> Privacy concerns may drive older and senior college members away from FB. Even high privacy concerns, are not driving undergraduate students away from it. Non-members have higher generic privacy concerns than FB members… Those users who join the network would not be more likely to exclude personal information from visibility if they have high privacy concerns... We detected little or no relation between participants’ reported privacy attitudes and their likelihood of providing certain information, even when controlling, separately, for male and female members.
> … a number of different reasons for the dichotomy between FB members’ stated privacy concerns (high) and actual information hiding strategies (mixed, but often low also for members with high stated concerns). Those reasons include peer pressure and unawareness of the true visibility of their profiles. (Acquisti and Gross 2006, 47-52)

CEU eTD Collection

It is important to emphasize the second reason the authors mention: unawareness of the true visibility of their profiles, which can be treated as another evidence that transparency-and-choice has failed. (Nissenbaum 2011,). In the previous section of this paper I argued that privacy concerns did not arise among Facebook users until the introduction of News Feed, something that made privacy settings visible. Also for some users it made it necessary to invest time and effort to adjust those settings according to their understanding of privacy. Despite the fact that the architecture of the site is far from obvious and transparent, which goes in direct contradiction with Facebook principles, this problem cannot be solved by providing more information on privacy protection techniques, since it cannot be protected from both the web-service owners and the state.

A common misperception of privacy and visibility adjustment practices is that the majority of the audience is careless. Fuchs criticizes the age-related reading of privacy matters, where young people are perceived as victims of misunderstanding of the terms of privacy as compared to older people: ‘One problem of the victimization discourse is that it implies young people are stupid, ill informed, that older people are more responsible, that the young should take the values of older people as morally superior and as guidelines. (Fuchs 2009, 13) Agreeing with Fuchs, I argue that privacy issues should not be subject to fallacy of misreading or misperceiving. As I previously noted above, young people use social networks to connect to people who share common interests and are concerned with privacy issues to that extent. A well-defined privacy policy should impose data protection requirements not on those who share it, but on those who gather, store and use it. As Fuchs argues in one of his later works, when sharing information online, users participate in content creation, however, they do not own this content, since it stays in the mediated terrain, therefore, this content has to be protected by intermediaries in the form of social media. (Fuchs 2011, 9)

As the majority of Facebook users are teenagers and students (since Facebook was founded as a campus network), they might not be of primary interest to surveillance structures. At the same time, since the responsibility for protecting privacy lies on the users, the state can request personal information that is stored on the Facebook servers for undefined period of time. As it happened during, for instance, the Twitter revolution, the authorities used social networks profiles to identify activists. Facebook and Google claim that the information

CEU eTD Collection

they provide to the third parties has been cleared of any identifying features (Facebook 2011, Google 2012). However, as Morozov suggests, “[One] 2009 study conducted by researchers at the University of Cambridge, … found that based on the limited information that Facebook discloses to search engines like Google, it is possible to make accurate inferences about information that is not being disclosed.” (2011, 158) Considering the fact that Facebook also stores log information which can be linked to individual IP addresses, state authorities, if needed, will have no difficulty in identifying individuals.

As the main function in Facebook’s profit-generating concept is targeted advertizing and not assistance to state surveillance, it can be expected that the information on data-handling practices will be present in the Terms of Use. However, in the Terms dated April 26, 2011 it does not explicitly state how the information can be used for commercial purposes. This new concern with commodification of personal data overshadows the concern with privacy issues in the media. When commercial agenda of Facebook was revealed, many users were outraged along with public figures who criticized Zuckerberg for building the social network guided by the principles of transparency that in fact became the most profitable business enterprise without its participants knowing how their data were used.(boyd 2008) Though according to the founder, it was not meant to be a commercial enterprise. (BBC, 2011). Christian Fuchs in his study of Facebook and other social networking sites provides an extract of its terms and conditions dated 2008:

> By posting User Content to any part of the Site, you automatically grant, and you represent and warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose, commercial, advertising, or otherwise,[6] on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing. (Facebook Terms of Use, accessed on November 2, 2008).

CEU eTD Collection

[6] My underlining throughout the text.

The previous account of terms of use explicitly emphasized the commercial use of the data collected. Therefore there is no legal ground for discontent. At the same time, moral context of commercial use of the data suggests that this change in the Terms might be attributed to mass discontent and outrage. Though, many users felt vulnerable and offended by the intrusion of the social network they did not withdraw from using the network. In other words, filtering out the information that can be made public is the easily available solution, but it does not solve the problem of unregulated issue of online privacy. Referring to the contextual approach proposed earlier in the thesis, the issue of privacy regulation has to be regulated officially. A solid legal framework should be provided and secured by the state that will enforce responsibility and accountability on the online intermediaries in cases when personal data is disclosed.

3.2.4. Common patterns of data collection and usage of Facebook, Google and Twitter

Concerns about privacy and commercial handling of personal data discussed above in relation to Facebook are equally applicable to Google and Twitter. However, compared to its fellow companies, Twitter has the least information on its users, since it operates in short 140-symbol messages in form of links to pictures or websites, and the most user-friendly privacy policy. At the same time Facebook provides an environment that is the most conductive of personal information dissemination. This pattern might change due to the recently introduced Google feature G+, new social networking platform. All three platforms use targeted advertizing, therefore transferring user data to the third parties.

CEU eTD Collection

In negotiating personal data transfer with the third parties, it is important to know the principles and standards that guide these practices. According to Nissenbaum, “there are certain brands of free-market capitalism make it easy to confuse the quest for profit with the pursuit of internal standards of excellence.” (Nissenbaum 2011, 42) When Sergey Brin and Larry Page first launched the Google search engine, they regarded commercial influences as contrary to a search engine's core mission as a performance-driven tool serving individuals' interests in locating information on the Web. In 1998, they wrote "The goals of the advertising business model do not always correspond to providing quality search to users… We believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm. (Brin & Page 1998) In the meantime, the company's 2011 annual report states that "ads are just more answers to users' queries." (FairSearch.org 2012) This change of rhetoric can be interpreted as the empowering effect of the increasing role of private intermediaries, whose influence is becoming more political.

Apart from the targeted advertising based on personal preferences aggregated by Google, the company has expressed a commitment to maintaining a barrier between identifiable search records and other records it accumulates with user profiles. As in the previous example of the change of rhetoric, the commitment can be revoked at any moment, as was Google's commitment to forgo behavioral advertising. (Nissenbaum 2011, 43) Therefore, the standards that usually guide businesses are applicably only as far as the circumstances preferable or acceptable for all the actors involved in the deal. In the case of Google, the state and the company have legal commitment that allows Google to offer its services to the public at the cost of personal information and grants the authorities access to this information upon request. However, there are no legal commitments between the public and the company. This issue is addressed only symbolically in the privacy policy of Google:

> We regularly review our compliance with our Privacy Policy. We also adhere to several self regulatory frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly. (Google 2012)

All three companies, Google, Facebook and Twitter, provide links to Safe Harbor Framework site. They comply with the US-EU Safe Harbor Framework and the US-Swiss

CEU eTD Collection

Safe Harbor Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information from European Union member countries and Switzerland. All three corporations have current certification status, but only Twitter lists "Employee/Employment Data and Corporate Compliance Program Data along with off-line, on-line generated and stored information as objects of its data protection certification. (Safe Harbor 2012)

Adherence of all three actors to the Safe Harbor framework can be considered as demonstrating the willingness to comply with certain norms, however, the substantially symbolic meaning of this certification cannot be regarded as legal regulation. At the same time, this certification and compliance with the certification requirements only outlines the information protection between the citizen of the US, EU member-states and Switzerland. There are no references to sources of regulation of information flows from and to the citizens of other countries.

All three web sites notify their users when they make changes to their privacy policies. Google comments: "We will post any privacy policy changes on this page[7] and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). The significance of the changes is decided in a self-regulatory manner which again pinpoints the flaws of notice-and-consent privacy policies.

An immediate reaction to privacy concerns from the realist perspective is that we need to filter out the information that we want to make public. However, the present research emphasizes that if the information can be made invisible to certain users, it still stays in the system and can be retrieved upon request. The question whether our personal information when processed and disassociated with the name should be treated as non-identifiable is subject to doubt because of the techniques that are at the disposal of both private

CEU eTD Collection

[7] http://www.google.com/intl/en/policies/privacy/

intermediaries and the state. The main concern, raised in this chapter, is that both private corporations and public officials engage in Internet surveillance, but both act out of different incentives. But what is more important is that this issue is currently not regulated. While state surveillance in some cases can be justified by the claims of the terrorist threat, there are no legal grounds to perform Internet surveillance through social networks, where most of the users are unaware of such privacy violations.

CEU eTD Collection

Conclusions

In addressing the question of how information flows should be regulated in the online environment and how this regulation fits into the perspective of free and open Internet, I have analyzed state and international legislation to conclude that it focuses on the regulation of intellectual property protection in most of the cases, but fails to provide effective legal frameworks to promote cyber security. In dealing with online privacy I proposed to employ contextual approach that emphasizes the necessity to define specific contexts in which informational norms of offline practices may be extended to corresponding online activities.

Other findings suggest that the changing dynamics of the state-public relations indicate the weakening of direct communication between the state and the public, at the same time emphasizing the role of private intermediaries. The implications of these findings for the civic engagement show that public sphere has migrated online and the reach of public opinion is limited largely to the Internet environment. In the absence of adequate regulation of online privacy states also do not address the regulation of relations between the intermediaries and the public in the context of personal information flows. For now, internet services such as social networking are offered on the basis of informed consent. This means that vast amounts of personal data that are used for benefit-generating commercial purposes are protected neither by the state nor by any international regulatory body.

As the findings of the thesis indicate, the notion and the implications of self-regulation in the sphere of privacy are highly problematic. Symbolic meaning of linking the conditions under which intermediaries gather and process personal data to international certification entities indicates the need for state regulation, rather than leaving issues of privacy to self-regulation. So far personal information flows over the Internet remain unregulated, but with regards to, for instance, cyber terrorism or crimes committed in an online environment, the urgency with which states are pressing for approval and enforcement of such acts as SOPA

CEU eTD Collection

and PIPA is understandable. Social movements who use Internet services to organize their actions and who suffer the most from state surveillance, especially in oppressive regimes, need adequate Internet regulation the most.

The proposed implementation of the contextual approach to the regulation of privacy online and information flows more broadly stands out in a sharp contrast to other approaches and if employed by policy makers can show decisive results in preventing commercial use of personal information and strict adherence to protection of human rights. The adoption of this approach can facilitate critical discourse within the public sphere and encourage renewal of state-public interaction and fruitful dialogue.

The present research provided a methodological context for addressing the issue of regulation of information flow and privacy on the Internet within the changing dynamics of the relations between the public sphere and the state. The major trends and difficulties in addressing the Internet regulation indicate that though the states remain the only legitimate actors in the process of law framing and implementation, their reluctance to communicate with the public signals the growing weakness of the state as a just and democratic decision-maker.

The limitations of the findings of this thesis are contingent on the destabilization in the state-public interaction discussed earlier. The relevance of the findings can be strengthened in the case when states recognize the need to foster public discourse when addressing socially important issues like the Internet regulation and privacy protection and abandon global terrorism-threat agenda. However, in case the growing alienation between the public and the state persists, entailing failed communication between them, the theory of contextual integrity will not be among the tools of more assertive policy-making.

CEU eTD Collection

References

Acquisti, Alessandro & Gross, Ralph. 2006. *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook.* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf

Anti-counterfeiting Trade Agreement (Accessed on May 18, 2012) http://register.consilium.europa.eu/pdf/en/11/st12/st12196.en11.pdff

Ammori, Marvin. 2011. Controversial Copyright Bills Would Violate First Amendment. http://ammori.org/2011/12/08/controversial-copyright-bills-would-violate-first-amendment-letters-to-congress-by-laurence-tribe-and-me/ (Accessed on May 22, 2012)

Barber, Benjamin R. 1999. 'Three scenarios for the future of technology and strong democracy.' *Political Science Quarterly*. 113: 573-590.

boyd, danah. 2008. *Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence*. Convergence: The International Journal of Research into New Media Technologies. Sage Publications. London, Los Angeles, New Delhi and Singapore Vol 14(1): 13–20

boyd, danah and Nicole B. Ellison. 2011. *Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies.* Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society".

Brin, Sergey. & Page, Lawrence. The Anatomy of a Large-Scale Hypertextual Web Search Engine. *WWW/Computer Networks* 30 (1–7) (1998): 107–117. (accessed on May 31, 2012) http://infolab.stanford.edu/~backrub/google.html

British Broadcast Corporation. 2011. Inside Facebook. http://www.youtube.com/watch?v=zeOlO_2nddY

Calabrese, Anrew. 2005. Communication, global justice and the moral economy. In *Global Media and Communication* 1(3), pp. 301-315

Calhoun, Craig. 2002. *Information technology and the International Public Sphere.* International Sociology Association, Brisbane, Australia. http://www.nyu.edu/calhoun/files/calhounInformationTechnologyAndThePublicSphere.pdf

Castells, Manuel. 2008. The New Public Sphere: Global Civil Society, Communication Networks and Global Governance" in *The ANNALS of the American Academy of Political and Social Science*, 616(1), pp. 78-93

Chandler, David. 2009. The Global Ideology: Rethinking the Politics of the 'Global Turn' in IR. *International Relations*, 23(4), pp. 530-547

CEU eTD Collection

CNet News. 2011. Europe rules ISPs can't be forced to block pirate sites. http://news.cnet.com/8301-1023_3-57331041-93/europe-rules-isps-cant-be-forced-to-block-pirate-sites/ (Accessed on May 18, 2012)

Comstock, Donald E. 1994. *A Method for Critical Research*, in Martin, Michael and McIntyre, Lee C. (eds), *Readings in the Philosophy of Social Science*. Cambridge, MA: The MIT Press, pp. 625–639.

Cottle, Simon. 2011. Media and the Arab uprisings of 2011: Research notes. *Journalism.* http://www.contexting.me/files/CottleMediaandtheArabUprising.pdf

Deacon, David. et al. 1999, Approaching Research. *Researching Communications,* Oxford University Press: New York

Deibert, Ronald J., Palfrey, John G., Rohozinski, Rafal & Zittrain, Jonathan. 2008. Access Denied. The Practice and Policy of Global Internet Filtering. Boston: MIT Press

Digital Millennium Copyright Act. Pub. L. 105-304. http://www.gpo.gov/fdsys/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf (Accessed on May 25, 2012)

Drake, William. & Wilson III, Ernest.J. 2008. *Governing Global Electronic Networks. International Perspectives on Policy and Power*. Cambridge, MA. MIT Press

Dwyer, Catherine, Starr Roxanne Hiltz & Katia Passerini. 2007. *Trust and privacy concern within social networking sites. A comparison of Facebook and MySpace*. In Proceedings of the 13th Americas Conference on Information Systems. Redhook, NY: Curran.

EU Commission Factsheet, November 2008. (Accessed on May 25, 2012) http://trade.ec.europa.eu/doclib/docs/2008/october/tradoc_140836.11.08.pdf

FairSearch.org. 2012. May 1st, 2012 Google's "Don't Be Evil" Hoax Continues: Paid Inclusion Blurs "Lines Between Ads And Search Results".Accessed May 31, 2012 http://www.fairsearch.org/deceptive-display/googles-dont-be-evil-hoax-continues-paid-inclusion-blurs-lines-between-ads-and-search-results/

Fuchs, Christian. 2009. Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance. Forschungsgruppe Unified Theory of Information (Research Group Unified Theory of Information). Salzburg and Vienna, Austria. http://www.icts.sbg.ac.at/media/pdf/pdf1683.pdf

Fuchs, Christian. 2010. Global media and global capitalism. In Indigenous societies and cultural globalization in the 21st century. Is the global village truly real?, ed. Nnamdi Ekeanyanwu and Chinedu Okeke, 556-594. Saarbrucken: VDM

Fuchs, Christian. 2011. A Contribution to the Critique of the Political Economy of

CEU eTD Collection

Google in *Fastcapitalism* 8(1). http://fuchs.uti.at/wpcontent/ uploads/Google_FastCapitalism.pdf

Habermas, Jürgen. 1989. *A reader on politics and society*. Edited by Steven Seidman. Beacon press. Boston.

Hafez, Kai. 2007. Theory – Structural Transformation of the Global Public Sphere?" in Hafez, K., *The Myth of Media Globalization*, Cambridge and Malden, MA: Polity Press, pp. 7-24

Herrera, Geoffrey. L. 2005. Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. 23-25

Kobrin, Stephen J. 2002. Economic Governance in an Electronically Networked Global Economy. In Rodney Bruce Hall and Thomas J. Biersteker eds., *The Emergence of Private Authority in Global Governance*. New York: Cambridge University Press, pp. 43-75.

Lohmann, Susanne. 2003: 'Representative Government and Special Interest Politics (We Have Met the Enemy and He is Us)', *Journal of Theoretical Politics* vol.15: 299-319.

McLuhan, Marshall & Fiore, Quentin. 1996. The Medium is the Massage. An inventory of effects. Produced by Jerome Agel. San Francisco: Hardwired

Morozov, E. 2009. Texting towards Utopia. Boston Review. March/April 2009. http://bostonreview.net/BR34.2/morozov.php

Morozov, E. 2011. The Net Delusion: the dark side of Internet freedom. New York, NY: PublicAffairs, 2011. 1st ed.

Mueller, Lawrence. 2010. Networks and States: The Global Politics of Internet Governance London: MIT Press , 2010 . 313 pp in Political Studies Review. P. 115 http://onlinelibrary.wiley.com/doi/10.1111/j.1478-9302.2011.00251_19.x/pdf

Norris, Pippa. 2000. Democratic Divide? The Impact of the Internet on Parliaments Worldwide http://www.hks.harvard.edu/fs/pnorris/Acrobat/apsa2000demdiv.pdf

Nissenbaum, Helen. 2011. A Contextual Approach to Privacy Online. Daedalus 140 (4), Fall 2011: 32-48. http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf

Nye, Joseph S. Jr. 2011. The future of Power. New York: PublicAffairs

Price, Monroe E. 2007. Civil society and the global market for loyalties. Annenberg School for Communication Departmental Papers.

CEU eTD Collection

PROTECT IP Act of 2011, S. 968, 112th Cong. (Accessed on May 22, 2012) http://www.gpo.gov/fdsys/pkg/BILLS-112s968rs/pdf/BILLS-112s968rs.pdf

Raboy, Marc. & Padovani, Claudia. 2009. *Governing global electronic networks: international perspectives on policy and power* / edited by William J. Drake and Ernest J. Wilson, III.
Published London: MIT Press, 2009.

Raboy, Marc. and Padovani, Claudia. Mapping Global Media Policy: Concepts, Frameworks, Methods. 2010. (accessed on May 31, 2012)
http://www.globalmediapolicy.net/sites/default/files/Raboy&Padovani%202010_long%20version_final.pdf

Rash, Wayne. Jr. 1997. *Politics on the Nets: Wiring the Political Process*. New York: W.H. Freeman.

Rogers, Richard. 2010. Mapping Public Web Space with the Issuecrawler. C. Brossard and B. Reber (eds.), Digital Cognitive Technologies: Epistemology and Knowledge Society. London: Wiley, pp. 115-126.
http://www.govcom.org/publications/full_list/Rogers_Digital_Cognitive_Technologies_preprint_Wiley_2009.pdf

Safe Harbor. 2012. http://safeharbor.export.gov/companyinfo.aspx?id=15209

Stop Online Piracy Act, 112th Cong., Oct 26, 2011. (Accessed on May 22, 2012)
http://judiciary.house.gov/hearings/pdf/112%20HR%203261.pdf

Stanton, Richard. The continuing transformation of the public sphere: from Jurgen Habermas to Osama bin Laden" in *All News is Local*, McFarland & Co., Jefferson, NC and London, 2007

Thaler, H. Richard and Sunstein, R. Cass. 2008. *Nudge: improving decisions about health, wealth, and happiness.* Yale University Press

Volkmer, Ingrid. 2003. "The global network society and the global public sphere", *Development*, 46(1), pp. 9-16

WSIS Tunis agenda 2005. http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

CEU eTD Collection