The Debate on the Moral Responsibilities of Online Service Providers

Mariarosaria Taddeo[1] · **Luciano Floridi**[1]

Abstract Online service providers (OSPs)—such as AOL, Facebook, Google, Microsoft, and Twitter—significantly shape the informational environment (infosphere) and influence users' experiences and interactions within it. There is a general agreement on the centrality of OSPs in information societies, but little consensus about what principles should shape their moral responsibilities and practices. In this article, we analyse the main contributions to the debate on the moral responsibilities of OSPs. By endorsing the method of the levels of abstract (LoAs), we first analyse the moral responsibilities of OSPs *in* the web (LoA_{IN}). These concern the management of online information, which includes information filtering, Internet censorship, the circulation of harmful content, and the implementation and fostering of human rights (including privacy). We then consider the moral responsibilities ascribed to OSPs *on* the web (LoA_{ON}) and focus on the existing legal regulation of access to users' data. The overall analysis provides an overview of the current state of the debate and highlights two main results. First, topics related to OSPs' public role—especially their gatekeeping function, their corporate social responsibilities, and their role in implementing and fostering human rights—have acquired increasing relevance in the specialised literature. Second, there is a lack of an ethical framework that can (a) define OSPs' responsibilities, and (b) provide the fundamental sharable principles necessary to guide OSPs' conduct within the multicultural and international context in which they operate. This article contributes to the ethical framework necessary to deal with (a) and (b) by endorsing a LoA enabling the definition of the responsibilities of OSPs with respect to the well-being of the infosphere and of the entities inhabiting it (LoA_{For}).

✉ Mariarosaria Taddeo
mariarosaria.taddeo@oii.ox.ac.uk

Luciano Floridi
luciano.floridi@oii.ox.ac.uk

[1] Oxford Internet Institute, University of Oxford, 1, St Giles, Oxford OX1 3JS, UK

Keywords Freedom of speech · Human rights · Levels of abstraction · Moral responsibilities · Online service providers · Privacy

Introduction

Among the private companies involved in the discussion on Internet governance, online service providers (OSPs)—such as AOL, Facebook, Google, Microsoft, and Twitter—play a crucial role. Since the emerging of Web 2.0, OSPs have become major actors, which significantly shape the informational environment (infosphere) and influence users' experiences and interactions within it. OSPs went from offering connecting and information-sharing services to paying members to providing open, free infrastructure and applications that facilitate digital expression, interaction, and the communication of information. This evolution has put OSPs in a peculiar position. For they often stand between the protection of users' rights and government requests, as well as shareholders' expectations. It is not a coincidence that some of the major OSPs—AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo—have joined forces and created the Reform Government Surveillance (RGS)[1] group to participate in the public debate on the regulation of Internet surveillance and the use of Information and Communication Technologies (ICTs) within governmental security strategies.

While there is a general agreement on the centrality of OSPs in information societies, there is still little consensus about what principles should shape OSPs' moral responsibilities and practices, over and above current legal requirements. These range from Google's generic motto "don't be evil" to much more specific guidelines concerning the protection of the public interest and the respect for basic democratic principles, e.g. openness, transparency, freedom of the Internet, security, and legal certainty, as identified in the 2011 G8 Deauville Declaration.[2] As a result, OSPs' efforts to act on societal issues are still problematic and often encounter shortcomings in design, implementation, and public recognition.

In this article we analyse the main moral responsibilities ascribed to OSPs during the past 15 years. In order to offer a systematic overview, we will look at OSPs' moral responsibilities using the method of the levels of abstraction (LoAs). This will enable us to distinguish OSPs' responsibilities on the basis of the different kinds of information that they control. Categories for Internet control have already been provided in the relevant literature. For example, Eriksson and Giacomello (2009) distinguish three categories of Internet control: access to the Internet, functionality of the Internet, and activity on the Internet. The latter ranges from filtering and blocking content online, and surveillance, to shaping the political and social discourse. OSPs' actions belong to the 'activity on the Internet'. However, within this category, OSPs control and regulate different types of data and information and

[1] https://www.reformgovernmentsurveillance.com.

[2] http://ec.europa.eu/archives/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf.

their responsibilities vary accordingly. The method of LoAs will help us to distinguish them.

Before proceeding, a brief introduction to the LoAs is required. Any given system, for example a car, can be observed by focusing on specific properties while disregarding others. The choice of these aspects, i.e. the observables, depends on the observer's purpose or goal. An engineer interested in maximising the aerodynamics of a car may focus upon the shape of its parts, their weight and the materials. A customer interested in the aesthetics of the car may focus on its colour and on the overall look. The engineer and the customer observe the same car at different LoAs. Thus a LoA is a finite but non-empty set of observables accompanied by a statement of what feature of the system under consideration such a LoA stands for. A collection of LoAs constitutes an interface. An interface is used when analysing a system from various points of view, that is, at varying LoAs. It is important to stress that LoAs do not have to be hierarchical (though they can be): the engineer's and the user's LoAs are not one higher or lower than the other. And note that a single LoA does not reduce a car to merely the aerodynamics of its parts or to its overall look. Rather, a LoA is a tool that helps to make explicit the observation perspective and constrain it to only those elements that are relevant in a particular observation for the chosen purpose (Floridi 2008).[3]

In this article, we will focus on two LoAs. One will highlight the moral responsibilities of OSPs *in* the web (LoA_{IN}), while the other will focus on moral responsibilities *on* the web (LoA_{ON}). The former pertains to the regulation of the content available online. LoA_{IN} highlights issues concerning information filtering, freedom of speech, censorship, and privacy. At LoA_{ON}, the focus shifts to the access to the metadata concerning users' activities online. To illustrate the distinction, consider that, given the two LoAs, the debate on the role of OSPs in collaborating with the US government within the PRISM program concerns OSPs' responsibilities *on* the web; while the discussion on OSPs' compliance with the request of the Chinese government to censor some of the information available online is about the responsibilities of OSPs *in* the web.

The analysis of the literature reveals that, during the past 5 years, increasing attention has been devoted to OSPs' public role and impact on contemporary societies (Fig. 1). OSPs are often seen as *information gatekeepers* (Calhoun 2002) (more on this in section "Managing Access to Information in the Web: Information Skewing"), for they control the information available online by making it accessible to the users (Shapiro 2000; Hinman 2005; Laidlaw 2008). This position ascribes a public role to OSPs. This is an unprecedented role for OSPs, which unveils new opportunities along with new problems and responsibilities that are profound and often require OSPs to align their goals with the needs of contemporary information societies (Madelin 2011). As Shapiro put it

[3] The reader interested in the methodology of the LoA may find useful the following books: (Heath et al. 1994; Diller 1994; Jacky 1997; Boca 2014). Philosophers interested in the concept of abstraction as used in this article may wish to see Hoare (1972).

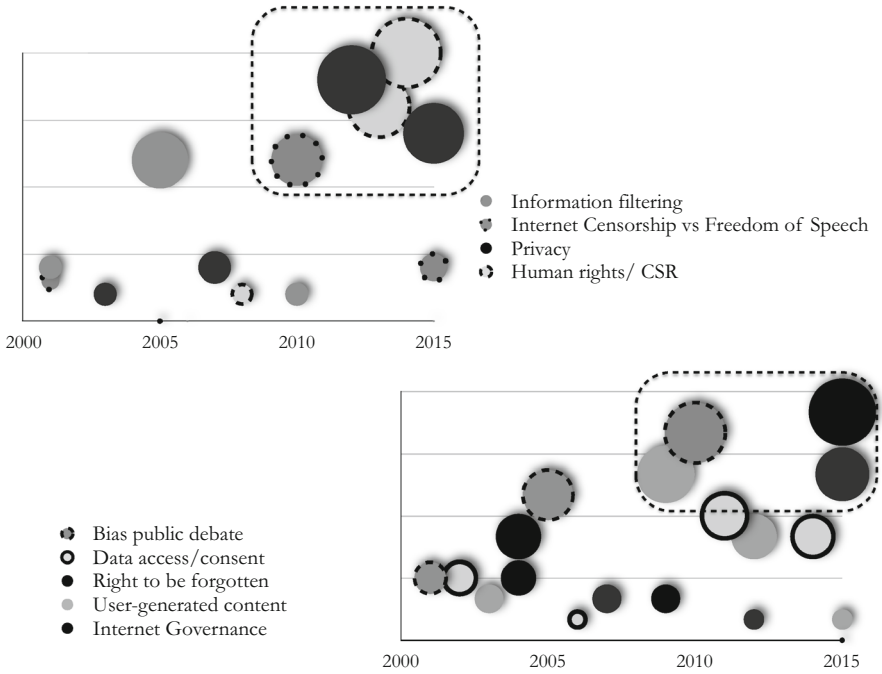

Fig. 1 The *two graphs* show some of the most relevant topics concerning the responsibilities of OSPs addressed in the literature in the past 15 years. The size of the *circles* is proportional to the number of research articles, books, and edited volumes that include either in the title or in the keywords one of the topics listed in the legends and which were published in the timespan indicated on the *x*-axis. While topics such as information filtering, user-generated content, and Internet governance have been central in the debate since 2000, other issues like OSPs' corporate social responsibilities and human rights, freedom of speech, and impact of OSPs on the public debate have attracted increasing attention in the past 5 years. The graphs have been produced using atlas.ti a qualitative analysis software and a database built with the references returned by WEB OF SCIENCE™ when searching for any of the topics indicated in the *graphs' legends*

> in democratic societies, those who control the access to information have a responsibility to support the public interest. […] these gatekeepers must assume an obligation as trustees of the greater good (Shapiro 2000, 225).

Given the international and multicultural contexts in which OSPs operate, the specification of their moral responsibilities will be effective—i.e. it will be regarded as ethically sound, appropriate, and desirable and offering a suitable guidance to shape OSPs' conduct by the different stakeholders involved in this scenario—only insofar as it will rest on an ethical framework able to reconcile the different ethical views and stakeholders' interests that OSPs face while acting as information gatekeepers. The analysis we propose in this article has the goal of laying the groundwork for such a framework, the definition of which has been left to a second stage of our research. Let us begin by considering OSPs' responsibilities at LoA_{IN}.

LoA_{IN}: Moral Responsibilities of OSPs in the Web

The analysis of OSPs' moral responsibilities with respect to the management of the content made available online has been a central point of research in different fields, including information and computer ethics, corporate social responsibilities and business ethics, computer-mediated communication, law, and public policy. Three topics are particularly salient in this debate: the organisation and managing of access to information; censorship and freedom of speech; and users' privacy. These topics have overlapping aspects and implications, which make it difficult to conceive a clear-cut separation of each issue. However, they also identify three important sets of ethical problems worthy of dedicated analyses.[4] In the rest of this article we will focus on each set separately. This slightly artificial structuring has the advantage of providing a conceptual map that will then allow the reader to identify the overlapping areas (Fig. 2) more easily. Let us begin by focusing on online information filtering.

Managing Access to Information in the Web: Information Skewing

The organisation and management of the access to information available online raises problems concerning the way in which search engines select and rank such information (Nagenborg 2005; Spink and Zimmer 2008; Tavani 2014). While the research on this topic initially focused exclusively on search engines, with the emergence of the Web 2.0 social networks and news aggregators also became objects of analysis, for these OSPs too can skew users' access to online information.

Introna and Nissenbaum's article (2006) is among the first publications on this topic. It analyses the role of search engines in defining the scope of access to online information and stresses the relation between such a scope and the development of a pluralistic democratic web. The article advocates diversity of the sources of information as a means to guarantee the fairness of information filtering processes and the democratic development of the Internet.[5] Both aspects can be jeopardised by the corporate, market-oriented interests of the private companies running indexing and ranking algorithms.

The article compares search engines to publishers and suggests that, like publishers, search engines filter information according to market conditions, i.e. according to consumers' tastes and preferences, and favour powerful actors. This promotes the so-called "rich gets richer" dynamic (Huberman 2003). For popular websites tend to be ranked higher hence acquiring even greater visibility.

[4] Dissemination and access to copyrighted material has also been a topic of great interest in research concerned with OSPs. However, this problem falls outside the scope of this article, for it has more to do with liability and the application of laws protecting copyright online than with the moral duties of OSPs. The interested reader may find useful the analyses of copyright online provided in Hanel (2006), Edwards (2011), Friedmann (2014).

[5] Other relevant contributions on the diversity of the sources and information available on the web have been provided in the literature in information and communication studies, law, and public policy. The interested reader may find useful the following articles: (Pandey et al. 2005; Pasquale 2006; Hargittai 2007; Van Couvering 2007; Diaz 2008; Hinman 2008; Lewandowski 2011).

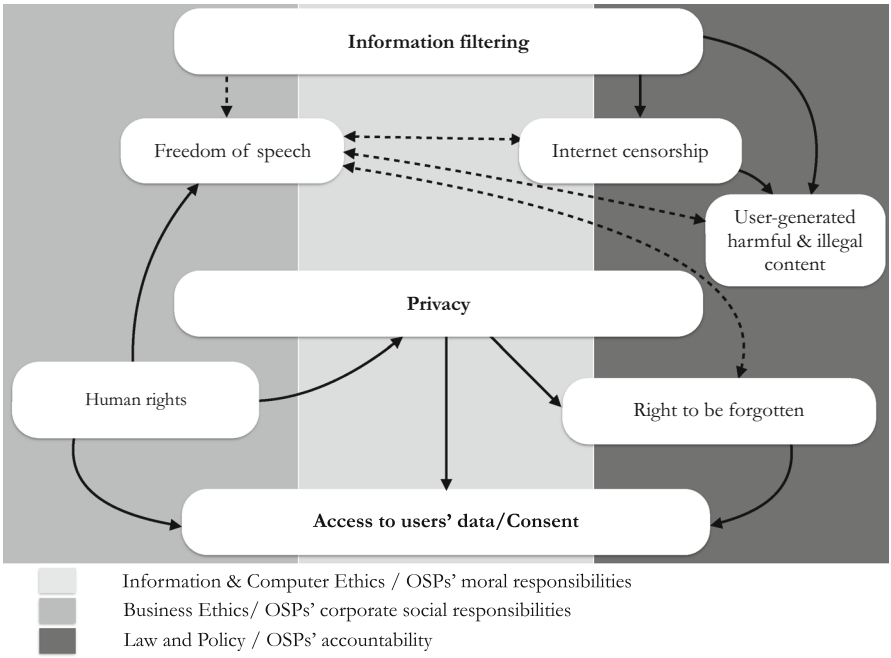

Fig. 2 This figure shows the key topics and the research areas in which the responsibilities of OSPs have been debated in the past 15 years. The *dotted arrows* indicate conflicting topics, while the *continuous arrows* link consistent topics. The direction of the *continuous arrows* signifies dependence relation between different topics, e.g. freedom of speech depends on the specification of human rights

Conversely, this system makes less visible those websites that are already poorly linked or visited and hence ranked lower. This dynamic prompts a vicious circle, which eventually leads to expunging niche, less renowned sources of information from the web, thus endangering the plurality and diversity of the Internet. Two corrective mechanisms are then suggested: embedding the

> value of fairness as well as [a] suite of values represented by the ideology of the Web as a public good (Introna and Nissenbaum 2006, 182)

in the design of indexing and ranking algorithms, and transparency of the algorithms used by search engines.

A different position on transparency of search and ranking algorithms has been prosed in Granka (2010).[6] The article points out that disclosing the structure of these algorithms would facilitate ill-intentioned manipulations of search results, while not bringing any advantage to the average non-tech-savvy user. Granka's paper also disputes the idea that market regulation of the Internet threatens the diversity of the information sources. On the contrary, it maintains that, in a market-regulated environment, companies will devote their attention to the quality of the search

[6] The reader interested in the transparency and the copyright of code will find interesting the following articles: (Reger 2004; Wolf et al. 2009).

results, which will have to meet the different needs and expectations of every user, thereby guaranteeing diversity of the sources and fairness of the ranking. In this respect, the article also objects to the analogy describing OSPs, search engines in particular, as publishers. Search engines

> parse through the massive quantities of available information […], the mechanisms whereby content is selected for inclusion in a user's search result set is fundamentally different than in traditional media—search engines universally apply an algorithm, whereas traditional news media makes case-by-case decisions (Granka 2010, 365).

The problem remains, however, when a search engine has a virtual monopoly and hence no real competition within a whole market, as it is currently the case for Google in Europe.

OSPs' editorial role is also analysed in Goldman (2006). The article describes search engine bias as a necessary consequence of OSPs' editorial work,

> to prevent anarchy and preserve credibility, search engines unavoidably must exercise some editorial control over their systems. In turn, this editorial control will create some bias (Goldman 2006, 119).

While the analysis recognises that such filtering may reinforce the existing power structure in the web and bias search results toward websites with economic power (Elkin-Koren 2001), it also advocates that the correction of search bias will follow from the fine-tuning of the search results with users' preferences. No extra moral responsibilities should be ascribed to OSPs in this respect. A similar position has also been expressed in Lev-On and Manin's and Lev-On's articles (Lev-On and Manin 2009; Lev-On 2009). The articles suggest that, given the huge amount of data filtered by search engines, unintentional exposure to diverse and non-mainstream information cannot be excluded. The issue then arises as to whether incidental exposure to diverse information may suffice to maintain an open, pluralistic web.

The personalisation of search results—offering diversified results based on the preferences of each individual, rather than those of the majority—has also been proposed as a remedy to the concerns highlighted by Introna and Nissenbaum. For the tailoring of search results leads to an organic refinement of searching and ranking algorithms so as to accommodate users' preferences and, at the same time, it makes it possible to correct the distortion performed by OSPs while fostering diversity in the sources and information circulating in the web. This is, for example, the argument proposed by both Goldman's and Crawford's articles (Goldman 2006; Crawford 2005).

The personalization of search results is not uncontroversial. Far from being seen as a solution to the problems engendered by information filtering, it has been objected to as a threat to democratic discourse in contemporary societies. In this respect, issues have been raised by several scholars (Sunstein 2001; Anderson 2008; Spink and Zimmer 2008; Pariser 2012). Custom-tailoring of search results challenges the basic underpinning of a deliberative democracy insofar as it undermines the possibilities of sharing cultural background and experiences and reduces the chances of being exposed to sources, opinions, and information that may

support or convey different world views. In particular, Sunstein's book (2001) criticises any approach relying on users' preferences and market dynamics to shape information access and communication:

> it is much too simple to say that any system of communication is desirable if and because it allows individuals to see and hear what they choose. Unanticipated, unchosen exposures, shared experiences are important too (Sunstein 2001, 131).

He argues that a custom-tailored access to information leads to a world fragmented into different versions of "the daily me" (Negroponte 1996),[7] in which each individual would be isolated in their *informational bubble* (Pariser 2012), from which conflicting views are excluded. A similar argument has also been proposed in Pariser's book (2012). The book criticises the personalisation of access to online information, because it promotes personalised *informational ecosystems* and *echo-chambers* that undermine the emergence and fostering of democracy.

Over the years, the discussion concerning the responsibilities of OSPs has moved from defining the measures that OSPs should deploy to correct their market bias and ensure a pluralistic web, to understanding the impact that OSPs have on the Internet as well as on the flourishing of democratic values and on societies at large (Fig. 1). This shift is partly due to the ideal of a democratic web inspiring the design of the Internet as a free, open network for the sharing of information (Toffler et al. 1995; Negroponte 1996; Diamond 2010). At the same time, the centrality of ICTs and in particular of the Internet in contemporary societies stresses the need to regulate access to online information so to protect and foster individual liberties and the democratic ideal. OSPs are major actors in this scenario, contributing to the shaping of both the informational environment and societies. For this reason, Sunstein's and Pariser's analyses ascribe to OSPs a civic responsibility to foster plurality and democracy.

Similar analyses leave unaddressed the identification of the principles that should guide OSPs when dealing with their civic responsibilities. Defining such principles proves to be a difficult task. OSPs are private companies to which academia, policy-makers, and society increasingly ascribe the role of *information gatekeepers*, generating the expectation that they will perform their tasks

> well and according to principles of efficiency, *justice*, *fairness*, and *respect* of current social and cultural values (McQuail 1992, 47) (emphasis added).

The notion of gatekeepers has been studied in business ethics, social sciences, and legal and communication studies since the 1940s. It characterizes those agents who have a central role in the management of resources and infrastructures that are crucial for societies. For example, in 1947, Lewin famously described mothers and wives as gatekeepers, for they were the ones deciding and managing the access and consumption of food for their families (Lewin 1947).

[7] Concerns for the implication that filtering of information may have for participative democracy and the nature of the web have also been expressed in Lessig (1999).

Metoyer-Duran (1993) offers a fruitful definition of gatekeepers according to which an agent is a gatekeeper if that agent

> (a) controls access to information, and acts as an inhibitor by limiting access to or restricting the scope of information; and (b) acts as an innovator, communication channel, link, intermediary, helper, adapter, opinion leader, broker, and facilitator.

Conditions (a) and (b) entail moral responsibilities, insofar as gatekeepers have a regulatory function. The private nature of gatekeepers, along with the responsibilities entailed by (a) and (b), is one of the cruxes generating the problems concerning their moral responsibilities (Freeman 1999; Black 2001).

Framing the discussion on the moral responsibilities of OSPs using the notion of gatekeepers unveils OSPs' public role, along with the accompanying friction that they may experience between corporate and public interests. However, this notion also risks biasing the discussion in an unfruitful way. Two major concerns arise in this respect.

The first concern emerges when considering the extant literature on corporate social responsibilities (CSR) (Crane et al. 2008), which focuses mainly on the duties towards societies that are inherent to the responsibilities of private companies having a gatekeeping function (Matten and Crane 2005; Palazzo and Scherer 2006; Scherer and Palazzo 2006; Albareda et al. 2007; Blowfield and Murray 2008; Okoye 2009; Helgesson and Mörth 2013). In this case, the analysis of the moral responsibilities is shaped by a deontological bias, addressing the moral duties that gatekeepers have *qua* controlling agents. This is not wrong *per se*. However, such a bias often leads to disregarding the rights of the *gated* (Barzilai-Nahon 2008), the receivers of the gatekeepers' actions, i.e. the *moral patients*.

The second concern arises from the attempt to overcome the first. In this case, users are usually identified as the ultimate moral patients. However, OSPs' gatekeeping function does not affect only users' online experiences, for OSPs' control over online information also makes them key agents shaping users' experience as well as the informational environment (Laidlaw 2010; Cerf 2011). The need then arises to define the moral responsibilities of OSPs with respect to both the users and the informational environment. Such a need becomes more pressing as one considers the extent of the control exercised by OSPs on the latter.[8] The regulation of user-generated content available online offers a good example of the case in point. The next section focuses on this topic.

[8] The issue arises as to whether OSPs should be ascribed moral responsibilities with respect to societies at large or solely with respect to societies depending on ICTs. The answer depends on the way such responsibilities are defined. For example, if one considers the protection of privacy a duty to respect human rights, then one could argue that OSPs bear this responsibility independently from the level of distribution of their services in a given region. One could also argue that societies where Internet is not pervasive will sooner or later become information societies and hence that, even if OSPs do not massively affect these societies, they will in the foreseeable future. We would like to thank one of the anonymous reviewers for pointing out this aspect.

Internet Censorship and Harmful Content

OSPs also manage access and circulation online of user-generated content. Part of this management implies preventing the dissemination of illegal content (e.g. child pornography), of hate speech, and of other material that may be deemed harmful to individuals and societies, e.g. pro-suicide, pro-anorexia or terrorism-promoting websites. Other forms of censorship may be prompted by governments to pursue political agendas beyond individual and social welfare.

Legally speaking, OSPs are generally not liable for the user-generated content that they host.[9] At the same time, OSPs have been encouraged to monitor and filter, to the extent that they can, the content circulating on the web (Hildebrandt 2013). Two main models have been endorsed to assess OSPs' liability with respect to third party content. The first one is the so-called "safe harbour" model.[10] In this case, the intermediary liability only applies to OSPs with respect to specific types of content, e.g. copyrighted material. In this model, OSPs are liable if they do not comply with the "notice and take down" procedure and hence do not act promptly to remove or disable access to illegal information when they obtain actual knowledge of such content. The second model guarantees broad immunity to OSPs by considering them as carriers of user-generated content for which they do not bear any liability, somewhat like a postal service. The question remains as to whether OSPs have any moral responsibilities to monitor and filter the web to prevent the dissemination of offensive and harmful material.[11]

Johnson has noted that, while it might be feasible to hold OSPs legally liable for the circulation of some contents, it would be much more difficult to argue that OSPs should be morally responsible for the behaviour of their users (Johnson 2009). This last point is quite uncontroversial, but it may also be misleading. The issue at stake is not whether OSPs should be held morally responsible for their users' actions. Rather, the problem is whether OSPs bear any moral responsibilities for circulating on their infrastructures third-party generated content that may prove harmful.[12] To some extent, similar responsibilities have already been ascribed to other media, like television and newspapers. Smoking advertisements have been banned in European countries because of their potential to induce harmful habits in their audience.[13] In this case, media are not held responsible for the actual smoking habits of the audience, nor are they held responsible for the tobacco industry's intention to promote smoking. But they are held responsible for the potentially harmful consequences of the information that they would disseminate.

Vedder's contribution (2001) delves into this issue and suggests that OSPs should be held morally responsible for the dissemination of harmful content. The article

[9] With the exception of countries like China and Thailand, where the strict liability model is endorsed and OSPs are liable for third-party content.

[10] For a critical analysis of the 'safe harbour' model see Pagallo (2011).

[11] An interesting analysis of OSPs' legal responsibilities with respect to this has been provided in Burk (2011).

[12] A legal analysis of third-party liability under US tort law has been provided in Ziniti (2008).

[13] http://ec.europa.eu/health/tobacco/law/advertising/index_en.htm.

distinguishes between *prospective* and *retrospective* moral responsibility and stresses that the two aspects go hand in hand. According to Vedder's analysis, OSPs are usually considered *prospectively* responsible insofar as they have the moral duty of avoiding possible future harm to their users. It is more problematic to ascribe *retrospective* responsibility to OSPs, for it presupposes guilt, and it has been maintained in the literature that such responsibilities cannot be attributed to communities or non-physical persons. However, Vedder's article argues that, since OSPs are considered prospectively morally responsible, they should also be held retrospectively responsible, and hence they bear full moral responsibility for the content that they circulate.

A similar position has also been supported in the analysis proposed by Tavani and Grodzinsky (2002). The article analyses the case of Amy Boyer, a young woman who was first stalked and then killed by Liam Youens, a man who used the web to collect information about the victim that was relevant to his plan.[14] Following Vedder's argument, the paper puts the burden of the responsibility for the information circulating online about the victim on both OSPs and the users who shared such information with the killer.

In a commentary, Cerf (2011) touched directly on the role of OSPs in preventing harmful uses of the web stating that

> it does seem to me that among the freedoms that are codified […] should be the right to expect freedom (or at least protection) from harm in the virtual world of the Internet. The opportunity and challenge that lies ahead is how Internet Actors will work together not only to do no harm, but to increase freedom from harm (Cerf 2011, 465).

Following Cerf's commentary, it may be desirable to ascribe moral responsibilities to OSPs with respect to the circulation of harmful material. However, this ascription raises further problems when considering the duties that these responsibilities may prompt, e.g. policing and filtering the content available online, and the possible breaches of individual rights, such as freedom of speech and information, and anonymity. This is a difficult balance to strike and to implement.[15] While OSPs should be held responsible for respecting this balance, and should be involved in the discussions aiming at striking a fair balance, it should not be their duty to define the balance and decide, for example, how much freedom of information can be sacrificed in the name of users' safety and security.

Reducing the harm on the Internet has put OSPs in a difficult position, standing between citizens' rights and expectations of a free, uncensored, access to information. OSPs are also caught in the friction between national and international powers. Some national powers, for example, seek to limit their citizens' right to freedom of speech and anonymity, while the international community recognises these as fundamental human rights. The next section analyses this problem.

[14] http://articles.latimes.com/1999/dec/05/news/mn-40632.

[15] Internet censorship and freedom of speech have also been at the centre of a debate focusing on the balance between individual rights and state power. This topic does not fall within the scope of this article. The interested reader may find useful (Taddeo 2013, 2014).

Internet Censorship and Freedom of Speech

In 2012, Internet freedom was declared a human right by the UN Human Rights Council, which called on states to promote and foster access to the Internet and to ensure that the rights to freedom of expression and information, as presented in Article 19 of the Universal Declaration of Human Rights, would be upheld online as well as offline.[16] Do OSPs have any responsibilities with respect to Internet freedom and with human rights in general? Some authors, like (Chen 2009), have argued that OSPs, and in particular social networks, bear both a legal and a moral responsibility to respect human rights, because of the centrality of their role on the web and of their knowledge of the actions undertaken by other agents, e.g. governmental actors, in the network. At the same time, both the Universal Declaration of Human Rights and the Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet (see footnote 12) mainly address states actors, making problematic the expectation that OSPs should be held responsible for respecting and fostering human rights (Karp 2009). This problem does not exclusively concern OSPs. It also involves several other private actors, especially those working in the international market (Anderson 2012), making this issue a central topic in the literature on business ethics. Consider, for example, the cases of human rights violations reported by Human Rights Watch concerning the energy industry, such as Royal Dutch/Shell's operations in Nigeria, British Petroleum in Colombia, and Total and Unocal's construction works in Burma and Thailand.[17]

Some authors, like Santoro and Brenkert, stress the need to consider the context in which companies act before assessing their moral responsibilities (Brenkert 2009; Santoro 1998). Santoro proposes a "fair share theory" to assess the moral responsibilities of multinational companies complying with the requests of an authoritarian state. According to this theory, the responsibilities for respecting and fostering human rights are ascribed differently depending on the capability of the company. Santoro poses two conditions for evaluating the capabilities of private companies and ascribing responsibility: (i) they have to be able to make a difference, i.e. change local government policies; and (ii) they have to be able to withstand the losses and damages that may follow from diverging from local governmental directions and laws. Both conditions highlighted in Santoro (1998) are problematic. Condition (i) offers a justification to any private company that may engage in immoral, or unlawful, actions. For the inability to make the difference in governmental policies allows the company to claim no moral responsibility for any violation of the human rights in which it may partake while collaborating or complying with a local government's directives. Condition (ii) does not stand as a valid requirement *de facto*, at least when considering major OSPs. For instance, in 2010 Google withdrew from China and still managed to be one of the most competitive OSPs in the global market. More recently, Facebook's CEO commented on this point stating that

[16] Resolution on "The Promotion, Protection and Enjoyment of Human Rights on the Internet" (Human Rights Council of the United Nations 2012).

[17] http://www.hrw.org/reports/1999/enron/.

> Today we're blocked in several countries and our business is still doing fine. If we got blocked in a few more, it probably wouldn't hurt us much either.[18]

Other scholars support a different view and hold private actors morally responsible for the protection and fostering of human rights (Arnold 2010; Cragg 2010; Wettstein 2012). The preamble of the Universal Declaration of Human Rights is often mentioned to support this point. It states that

> every individual and every organ of society, keeping this Declaration constantly in mind, shall strive by teaching and education to promote respect for these rights and freedoms […].[19]

The responsibility of all members of societies to promote respect for human rights has been remarked and further elaborated in the Declaration of Human Duties and Responsibilities (the so-called Valencia Declaration),[20] which focuses on the moral duties and legal responsibilities of the members of the global community to observe and promote respect for human rights and fundamental freedoms. The global community encompasses state and non-state actors, individuals and groups of citizens, as well as the private and the public sector. Private companies are also expressly mentioned as

> responsible for promoting and securing the human rights set forth in the Universal Declaration of Human Rights

in the preamble of the UN Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises.[21]

One of the cases about the moral responsibilities of OSPs and the respect of human rights (freedom of speech in particular) that has been most debated in the relevant literature concerns the complying of some OSPs, like Google, Microsoft, Yahoo!, and Facebook, with the requests made by the Chinese government on Internet censorship and surveillance.[22] OSPs have responded in different ways. Some, like Google (in 2010) and Yahoo! (in 2015), eventually decided not to comply with these requests and withdrew from the Chinese market. Others refer to the so-called consequentialist argument to justify their business in China. The argument was first provided by Google to support its initial compliance with the Chinese government requests. It holds that, while the Chinese people could not access some sources of information due to the local censorship, they could still use Google's services to access a whole lot more online information. In more sophisticated terms, it endorses the logic of a 'better than nothing' approach. More

[18] https://m.facebook.com/zuck/posts/10101974380267911.

[19] http://www.un.org/Overview/rights.html.

[20] http://www.unesco.org/bpi/eng/unescopress/1999/99-92e.shtml.

[21] The document has been approved on August 13, 2003 by the United Nations Sub-Commission on the Promotion and Protection of Human Rights. http://business-humanrights.org/en/united-nations-sub-commission-norms-on-business-human-rights-explanatory-materials.

[22] Governmental censorship has spread throughout the globe with the Internet; the literature on OSPs' responsibilities in China casts an interesting light on a problem that concerns several other countries around the world (Aceto et al. 2015).

recently, Facebook and Microsoft have proposed the same argument. As Facebook's CEO states

> I believe we have a responsibility to the millions of people in these countries who rely on Facebook to stay in touch with their friends and family every day. If we ignored a lawful government order and then we were blocked, all of these people's voices would be muted, and whatever content the government believed was illegal would be blocked anyway.[23]

Those who maintain that private companies ought to comply with human rights, because these are preeminent to local governmental actions, criticise the consequentialist argument.

> Multinationals […] should respect the international rights of those whom they affect, especially when those rights are of the most fundamental sort (Donaldson 1992, 68).

Such a position is also maintained in Dann and Haddow's article (2007), whose article ascribes moral responsibility to company executives, who make the final decisions and shape a company's conduct.A different account of the moral responsibilities of OSPs partaking in local governmental censorship has been provided in Brenkert's analysis (2009), where the notion of 'obedient complicity' is suggested,

> [t]his would occur when a business follows laws or regulations of a government to act in ways that support its activities that intentionally and significantly violate people's human rights (Brenkert 2009, 459).

The notion rests on the idea of permissible moral compromise. This is the compromise that agents make with themselves to forgo or even violate some of their moral principles to fulfil other, more important, values. OSPs operating in countries requiring Internet censorship face conflicting responsibilities towards different stakeholders, not just users, but also local employees and shareholders. For this reason, these OSPs may be justified in engaging in a moral compromise that may violate human rights, if this enables the achievement of more important objectives.

Brenkert's article proposes the so-called 'all things considered' approach to assess whether an OSP may be in a position to violate its moral principles or universal rights. The article considers the immediate context in which OSPs operate and the multiple responsibilities that this implies. For example, an OSP may be put in the position to compromise its moral values or to disregard human rights and comply with local laws lest its employees working in a given territory be held liable for the company's decision, or to avoid damaging the shareholders' interest. According to Brenkert's article, a moral compromise may be justified in these cases.

As any consequentialist approach, the 'all things considered' enables one to cover a wide range of responsibilities of private companies and assess them with regard to the company's maximum utility. This proves problematic, because the assessment of the moral responsibilities of a company depends on the scope of the

[23] https://m.facebook.com/zuck/posts/10101974380267911.

context that is being considered. Recalling the LoA methodology, let us assume that one endorses a LoA to identify the company's interest. In doing so, one may focus solely on the local interests of the company, the risks that the company may take in refusing to respect local laws, and the benefits that may follow from complying with the requests of local authorities. This LoA may support the acceptance of moral compromise and justification of the possible breach of human rights. However, such a LoA proves to be too narrow to consider properly the interest of a company operating in the international market, such a company needs to consider more factors than its local interests. It would be a LoA adopted according to the wrong purpose. A less restricted LoA—adopted for a better purpose—could account for observables such as the company's global reputation, the impact that breaching human rights may have on the company's public image, as well as the company's local interest. It would thus unveil the relevance of respecting human rights even when this may conflict with the interest of the shareholders. It follows that while the 'all things considered' approach was intended to mitigate the burden of OSPs' moral responsibilities, it actually offers one more argument in favour of OSPs' duty to respect and foster human rights.

The debate on the responsibilities of OSPs with respect to human rights highlights the challenges that come from the multicultural and international context in which OSPs work. It also shows the global relevance and impact that OSPs have on information societies. While it is increasingly less acceptable to maintain that OSPs, as private companies, are only responsible to their employees and shareholders, it is also problematic to ascribe to OSPs full responsibility for the fostering and respecting of human rights. For this entails that OSPs can arbitrarily and independently decide the circumstances and the modes in which they need to respect such rights.

Two aspects have been under-estimated in this context. One concerns the role and responsibilities of actors like the UN or the European Union in regulating OSPs' conduct so to ensure that they effectively respect human rights in their activities, independently from the geographic regions in which such activities are conducted. This is quite a problematic topic, for it prompts questions concerning sovereignty, Internet governance, and the territoriality of jurisdiction. However, as remarked in this section, international compliance of private companies with human rights is not a new problem and some legal international procedures are already in place to tackle it.

The second aspect concerns the definition of an ethical framework that can address the problems at hand. The analyses considered in this section identify in human rights such a framework. However, this has been shown to be insufficient, for human rights restrict the focus to human moral patients. As stressed in section "Managing Access to Information in the Web: Information Skewing", OSPs do not only affect human users, they also shape the informational environment. Overlooking OSPs' role within the environment that they build will impair any attempt to define their wider moral responsibilities towards the whole infosphere from an environment perspective. The risk is that the resulting analysis will be either too generic, i.e. OSPs should respect human rights in all circumstances, or too

narrow, i.e. OSPs' responsibilities concern exclusively human agents and only in some circumstances.

The time has come to consider OSPs' responsibilities with respect to users' privacy at LoA_{IN}.

OSPs' Responsibilities and User Privacy

The voluntary sharing online of personal information raises several concerns with respect to the protection of users' privacy.[24] For one thing, the personal information that is voluntarily shared online often exposes online and offline personas (Taddeo 2014) beyond the original intention of the users, leading to unforeseen breaches of their privacy and to potentially harmful consequences. Cyber-stalking (Tavani and Grodzinsky 2002) and the use of social networks to check employees' and students' backgrounds (Qi and Edgar-Nevill 2011; Semitsu 2011) offer good examples of said harmful consequences.

Responses to these concerns address both users' habits and OSPs' attitudes towards privacy. Some refer to the so-called "privacy paradox" (Acquisti 2004; Barnes 2006; Norberg et al. 2007; Rosen 2015) to stress that individuals continue to disclose personal details online, albeit being aware of the risks that this habit poses to their privacy. Qi and Edgar-Nevill caution that

> as social networking search and investigation become more popular, the public needs to know the processes and the rules regulating these activities. Understanding the extent of data disclosure on the social network is the first step for all (Qi and Edgar-Nevill 2011, 74).

At the same time OSPs, and particularly social networks, are considered responsible for a *de facto* devaluation of privacy, for they nudge their users to share more personal information using both open statements, see for example Sun Microsystems' CEO, McNealy "you have zero privacy anyway. Get over it",[25] and architectural design or apps like Facebook's newsfeed and Beacon (Baym 2011; Lanier 2011). In the rest of this section, we will review the moral responsibilities ascribed to OSPs with respect to users' privacy at LoA_{IN}.

An interesting contribution to this debate has been offered in Spinello's article (2011). The article rests on the understanding of privacy as an individual moral right, which OSPs have the moral responsibility to protect. Following the definition of privacy as "limited control of restricted access" to personal information proposed by Tavani and Moor (2001), Spinello's paper advocates the need to give users the power to control and limit access to the information that they share. OSPs would comply with their moral responsibility to protect users' privacy by endorsing a proactive approach and measures that would ensure users the maximum level of control over their personal information.

---

[24] For a review of the most relevant contributions of the debate on information privacy the reader may refer to Tavani and Moor (2001), Solove (2008), Smith et al. (2011).

[25] Mark Zuckerberg, Facebook's CEO, declared in 2010 that privacy is not a social norm any more as "people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people". http://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

The proactive approach mentioned in Spinello's analysis is recalled in Hull et al.'s paper (2011), which also attributes to OSPs moral responsibility to protect users' privacy at LoA_{IN}. This article relies on Nissenbaum's analysis of privacy (Nissenbaum 2010) and criticizes OSPs' architectures, in particular social networks, for treating human relations as if they were all of the same kind. OSPs' platforms would be better suited to managing users' personal information if they respected context-sensitive privacy norms, considering a greater array of social settings, rather than just focusing on the distinction between public and private. It is worth noting that, to some extent, this criticism has been taken seriously. Some social networks, e.g. Google+ and Facebook, allow access to a user's personal information to be curbed depending on the kind of social relations that they enjoy with other users.

The analyses provided in the previous articles rest on an understanding of the protection of privacy as an individual choice, i.e. a user only needs to apply high privacy settings when sharing her information to protect her right, and OSPs need to offer and facilitate such a choice. However, when one takes into consideration the interpersonal nature of information sharing in contemporary hyper-connected societies, this approach proves to be too narrow to be effective and to cast light on the parties who bear moral responsibility for protecting privacy. Even if a user has a highly protective privacy setting, personal information could be accessed by unauthorised parties due to the setting of other users in his/her network (Schwartz 1999; Caudill and Murphy 2000). This raises new problems, insofar as the difficulty of monitoring other users and uncertainty about their behaviours poses the need for a more refined privacy management.[26]

Two approaches have been proposed to overcome such difficulties. One, the *communitarian approach*, shifts moral responsibility for controlling information and protecting privacy from individuals to the community (O'Hara 2010; Xu 2012). The other, the *proxy approach*, focuses on OSPs and other major private and public actors, which can enforce social controls through regulation and codes of conduct (Smith et al. 2011).

The communitarian approach frames privacy as a public good, the benefits of which concern the community and not just the individuals. Following the analysis provided by Etzioni (1999), O'Hara's article (2010) maintains that privacy, as an individual right, may undermine community welfare if it is not properly curbed and balanced against other social concerns. The choice of some individual to share personal information online may be harmful not just to that individual, but to the community at large. Hence, according to this view, the right to privacy implies the duty of the single person toward the community to share responsibly and to monitor the flow of personal information circulating in their network. Individuals, as part of a community, need to agree on strategies for collectively managing the shared information, e.g. establishing a friendship-based model for privacy protection (Besmer et al. 2009), or rules of thumb regarding sharing with other users, such as asking for approval before disclosing content from those involved (Lampinen et al. 2011).

[26] Research on privacy breaches occurring because of third-party access and of users' habits have been provided in Brandimarte et al. (2013), Lampinen et al. (2011), Wang et al. (2011), Madden (2012), De Wolf et al. (2014).

Moral responsibility for the protection of individual privacy shifts back to OSPs when embracing the proxy control approach. In this case,

> people try by one means or another to get those who have access to resources or expertise or who wield influence and power to act at their behest to secure the outcomes they desire (Bandura 1999, 13).

OSPs bear responsibility because they are the depositaries of users' trust. Donaldson and Dunfee argue that there is an integrative social contract between users and OSPs (Donaldson and Dunfee 1999). Users provide their personal information to OSPs, which in turn offer some services to the users. One obligation, following this social contract, is that the OSPs accept the responsibility of managing consumers' personal information properly. This social contract rests on users' trust in the company's compliance with the contract. This trust is essential to overcome initial users' uncertainty and foster interactions online, and as such it is crucial for OSPs to preserve it (Weckert 2005; Taddeo 2010; Turilli et al. 2010). A significant difficulty is that the relation between users and OSPs seems to be modelled more on a version of a gift economy, which de-responsabilitises the gifter with respect to the giftee, rather than on any more or less metaphorical social contract (Floridi 2015a, b).

Trust in OSPs and the proxy approach have also shaped the application of the right to be forgotten in Europe, raising non-trivial ethical problems. The next section will delve into this issue.

The Right to be Forgotten and OSPs' Responsibilities

The so-called right to be forgotten was announced in Europe in 2012:

> if an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system (Reding 2012).

It has its roots in the French right of oblivion, which allows an individual to object to the publication of information about his/her criminal conviction, once s/he has served the sentence and been rehabilitated. As Mayer-Schönberger argues, this right is also rooted in the European history of the XX century, when the collection and retaining of personal information often turned out to be a powerful tool in the hand of totalitarian regimes. In post-1989 Europe, the possibility to be forgotten is seen as an extra measure fostering democracy and plurality (Mayer-Schönberger 2011).

If at first sight this right may seem an uncontroversial means to empower citizens to protect their privacy by ensuring them the control over their personal data, a more attentive analysis unveils the friction between this right and the right to freedom of speech and information. Striking the correct balance between the two is not a simple matter. Things change, for example, depending on which side of the Atlantic one is.[27] According to the European approach, privacy trumps freedom of speech; whereas the American view is that freedom of speech is preeminent with respect to

[27] An example of such a friction is discussed in section "LOAON: OSPs' Moral Responsibilities on the Web" with respect to the debate on the 'right to be forgotten'.

privacy (Rosen 2012). Hence, defining the responsibilities of OSPs with respect to the right to be forgotten turns out to be quite problematic, as it involves the balancing of different fundamental rights as well as considering the debate on the national versus international governance of the Internet (Floridi 2015a).

All these issues became evident with the ruling of the Court of Justice of the European Union (CJEU), which, in May 2014, decided that, given some circumstances, Google (or any other search engine operating in Europe) must remove from its search results the links to personal information if this is "*inaccurate, inadequate or no longer relevant*"(emphasis added).[28] The ruling opened a Pandora's box,[29] because anyone who thinks it inappropriate for some information concerning their personal life to be accessible online can now ask Google to delist it from its search results (note that the information would not be removed from the web, despite what it is indicated in Reding's quotation above).

According to European regulation, OSPs that are presented with a request to remove personal information "shall carry out the erasure without delay", unless the retention of the information is deemed essential for the right of freedom of expression. This ascribes to OSPs the responsibility to assess, on a case-by-case basis, the legitimacy of the sharing of the personal information online and to decide at which point the delisting of such information would be a case of undue censorship. Having to define the criteria for deciding which delisting requests to approve, Google sought the advice of a pool of international experts, who suggested a set of principles that should guide it in complying with the ruling of the CJEU.[30]

Very briefly the council advised Google to (a) apply the delisting decision across all its European websites (e.g. Google.de, Google.it, Google.es and so on), and (b) to notify publishers when a delinking procedure was initiated. Four more criteria were offered to guide Google in assessing the delisting requests: (i) evaluate the public role of the data subject, (ii) consider whether information to be delisted may impact private or public interests, (iii) consider the source of the information, and finally (iv) the timeframe of information was suggested as a criterion to assess its relevance. Both the suggestions and the criteria proposed by the advisory council unveil the responsibility to *judge* the information in question ascribed to Google and to several other OSPs (both Yahoo! and Microsoft have set forms available online to allow users delisting request) by the ruling of the CJEU.

The judging role of OSPs is controversial. For example, Rosen argues that, in this way, the power and responsibility of making public decisions shifts from judicial courts to private actors (Rosen 2012). The public role of OSPs in contemporary societies is undeniable, and so is the need to ensure that OSPs will act consistently with the public good (the reader may recall the discussion on the responsibilities of OSPs as information gatekeepers in section "Managing Access to Information in the Web: Information Skewing"). Yet, the application of the right to be forgotten goes a step too far. It does not ascribe to OSPs the responsibility to *act* by respecting the

[28] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

[29] Julia Powles maintains an extensive bibliography online at http://www.cambridge-code.org/googlespain.html.

[30] Disclosure: one of the authors of this paper (L. F.) is a member of the Advisory Board.

criteria for protecting and fostering individual rights as well as societies' moral principles and welfare. It puts OSPs in the position to have to *decide* about those criteria and those principles and their implementation. Hence, OSPs become both "*the judge and the jury*".[31]

As remarked in Gerry and Berova (2014), the ruling started a privatization of the judging power, which poses issues of transparency and accountability. OSPs, being private companies, do not have to comply with the same standards that apply to public institutions, nor are they expected to disclose any information about how they comply with the court's order. Yet absence of transparency and accountability risks paving the way to corruption, arbitrary decisions, and unfair applications of the ruling of the CJEU. Even more importantly, while the ruling may strengthen individuals' control over their personal information at LoA_{IN}, it does not do much to reinforce an individual's control at LoA_{ON}, that is, on the access that third party, e.g. corporate or government agents, may have to their data trails.

The reader may recall that, in section "Introduction", we mentioned the RGS group as an example of the reaction of OSPs to the difficult position in which OSPs find themselves. The RGS group signed a letter to the US President and Congress asking them to endorse five principles in revising US surveillance policies: limiting government authority in assessing users' data, oversight and accountability, transparency, respect for the free flow information, avoiding conflicts among governments.[32] The RGS group and its principles are OSPs' response to the debate prompted by the Snowden revelations on PRISM, the NSA massive surveillance programme. The PRISM scandal raised significant concerns internationally about surveillance in information societies. Most of the analyses developed on this topic frame the problem as the balance of surveillance and security with individual rights (Taddeo 2013). One crucial way in which such a balance is achieved is by regulating access to users' data. When considering this aspect, problems arise with respect to OSPs' role and responsibilities as information gatekeepers. The next section focuses on this topic.

LOA_{ON}: OSPs' Moral Responsibilities on the Web

In this section, we shall adopt the LoA_{ON} to consider OSPs' responsibilities in managing access to users' data.[33] In contemporary information societies, data are a crucial, resourceful asset, which can drive and support the economy, industry, scientific research, welfare as well as governance, surveillance, and security. Regulating access to data is not a trivial matter, as it involves balancing societal interests and progress with individual rights. Privacy plays a crucial role in this

[31] http://www.telegraph.co.uk/technology/google/10967211/Google-is-the-judge-and-jury-in-the-right-to-be-forgotten.html.

[32] https://www.reformgovernmentsurveillance.com.

[33] Net neutrality also refers to responsibilities on the web. However, this problem concerns the backbone infrastructure of the web and hence it involves Internet Service Providers more than Online Service Providers. The interested reader may find useful the following articles: (Blumenthal 2001; Lessig 2007; Schahczenski 2008; Turilli et al. 2012).

context, for users' data trails are quite revealing of their tastes, health, finance status, and social interactions. OSPs often stand between individuals' personal data and powerful agents aiming at gaining access to such data, e.g. governments as well as private companies, and OSPs themselves have a strong interest in collecting and mining users' data. The question then arises as to what principles should regulate access to users' personal data and information and what should OSPs' responsibilities be in accessing, controlling, and managing users' data.

Different positions have been held in the relevant literature in this respect. Some see in OSPs the depositary of users' trust. As such, OSPs have the responsibility to respect individual rights while managing their data (Donaldson and Dunfee 1999). Others strengthen this view by referring to a duty of *loyalty* of OSPs toward their users (Kerr 2002). The duty of loyalty demands that parties remain faithful to each other even when conflict arises between the interests of the peers. Kerr's article provides four criteria to identify those relationships in which the trusted party has a duty of loyalty to the trusting one: (i) if the former has some discretion or power and (ii) can unilaterally use this power to affect the trusting party, (iii) if the trusting party is vulnerable and/or at the mercy of the party holding the power, and (iv) if the trusting party is entitled to expect that the trusted party will act in her interest. Kerr's paper maintains that the relationship between OSPs and their users satisfies all four conditions. Condition (iv) is quite interesting, for it stresses a point that has also been highlighted in an opinion published by the Article 29 Working Party (Art. 29WP),

> [users] usually have an expectation about the purposes for which the data will be used. There is a value in honoring these expectations and preserving trust and legal certainty.[34]

Users' rights and *expectations* that users have about those rights play a central role in the regulation of data access developed during the past three decades as well as in the definition of OSPs' responsibilities at LoA_{ON}.

More recently, however, both academics and policy makers have criticised the effectiveness of focusing exclusively on users' rights when assessing data management (Acquisti and Grossklags 2005; Jolls and Sunstein 2005; World Economic Forum 2012; Cavoukian 2014; Cate et al. 2014; Kiss and Szőke 2015). The keystone of the criticism is the "notice and consent" model. The model rests on the assumption that users give consent to the treatment of their personal data after having read carefully the notice of each service to which they subscribe. However, this model ceases to be effective in contemporary societies. On the one hand, the more individuals use ICTs in their daily practises, the higher the number of privacy notices that they are expected to read, and the less attention users devote to the notice. On the other hand, the "notice and consent" model basically offers a Hobson's choice[35] and stands between the users and the services they want to access. Thus, in order to access a given service, users may unintentionally consent

[34] Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation", p. 4.

[35] This is a free choice in which only one option is offered, so it is really equivalent to a 'take it or leave it' choice.

to types of data processing that in reality they do not want. Schermer et al. (2014) refer to the "crisis of consent" to indicate a phenomenon that has led the notice and consent model to be devoid of the role originally attributed to it.

An attempt to address this crisis of consent has been provided in 2013, when the Organisation for Economic Co-operation and Development (OECD) published an updated version of the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD 2013). The guidelines were first implemented in 1980.[36] Since then, they have provided a common ground for national and international regulation of data access. The main problem addressed by the guidelines is the protection of user privacy. The main goal is to avoid users experiencing any physical or moral harm due to third-parties accessing their data. The update of the OECD guidelines has set a watershed in the definition of duties and responsibilities in managing users' data, given the 2013 version switched the focus from users' rights to the duties of data stewards [data controllers and data users, (Cate et al. 2014)], with an entire new section (Part three) devoted to guide data stewards in implementing the accountability principle. The principle states that "a data controller should be accountable for complying with measures which give effect to the principles stated [in section two]" (OECD 2013, 15), data stewards respect the principle if they meet the following three requirements: deploy privacy management procedures; can demonstrate that such procedures are appropriate; notifies the relevant authorities if and when a security breach affecting personal data occurs.

This shift fuelled the debate on the responsibilities of data stewards, e.g. OSPs, in contemporary information societies (Kiss and Szőke 2015).

In their report, Cate et al. (2014) defend this shift, arguing that it offers a better framework to fine-tune privacy with the different uses of data in contemporary societies. The report also stresses that (i) the responsibilities pertain to the processing of data rather than to obtaining consent from users, and that (ii) concern should be focused more on the use of the collected data than on the collection itself. Point (ii) rests on the observation that the context in which data may be used in the future, as well as the value that they will have, is often unclear or unforeseeable at the moment of the collection. It is then the responsibility of data stewards to ensure that users' data will be processed in a way that respects individual rights—such as privacy, anonymity, and transparency—even when used in contexts and for purposes that were not foreseen at the moment of the collection.

A different approach has been proposed in Cavoukian's article (2014). The article objects to the shift—from the rights of data subjects to the duties and responsibilities of data stewards—as being paternalistic and dangerous for the protection of privacy. The endorsement of privacy by design is suggested as an alternative method for managing data access so to respond to the needs of contemporary society without threatening users' privacy. According to Cavoukian's article, data stewards have the responsibility of implementing design measures that protect a user's privacy by default. In particular, the article stresses the value of de-

[36] A brief description of the history of the definition of international guidelines for the protection of privacy has been provided in Gerry and Berova (2014), Kiss and Szőke (2015).

identification methods, for they can protect individual privacy while exploiting the many benefits following from the use of personal data.

The OECD guidelines, Cate et al.'s report, as well as Cavoukian's analysis offer guidance for policy solutions to address the crisis of the 'notice and consent' model. These guidelines find their limit in the absence of a conceptual framework that can account for the role that both data and data stewards, and OSPs in particular, play in contemporary societies. Developing such a framework along with ethical analyses to define the principles shaping the conduct of data stewards are preliminary and necessary steps towards a fair regulation of data access and management.

Conclusion

In this article we have discussed the current literature focusing on the moral responsibilities of OSPs. We have highlighted that the role of OSPs as information gatekeepers, the corporate social responsibility that this role entails, and the respect of human rights, are topics that have become increasingly relevant during the past 5 years and across the three research areas of information and computer ethics, business ethics, and law (Fig. 1).

The academic interest in these topics stems from the pressing need felt by society to regulate OSPs' conduct in order to ensure the respect of the public good and the fostering of societal welfare. Such a need is often addressed by endorsing an *ad hoc* approach and by delegating to OSPs normative decisions. A good example of the case in point is offered by Google, which is currently both the "judge and the jury" with respect to the application of the right to be forgotten in Europe.

Given the relative novelty and the very significant relevance of the role that OSPs play in contemporary societies, it does not come as a surprise that attempts to regulate OSPs rests on an *ad hoc* strategy to tackle problems as they emerge while, at the same time, the debate on the legal requirements for OSPs' conduct identifies long term solutions. However, the definition of such requirements proves to be difficult when considering OSPs' gatekeeping function, the multicultural, international context in which they operate, as well as the interdependency of the services that they offer in different regions of the world. The latter is a specific feature of OSPs, which requires careful consideration, ethical foresight, and long-term planning. All this makes the attempt to regulate OSPs' conduct by endorsing an *ad hoc* approach unsatisfactory if not unfeasible. These problems can be overcome once legal analyses rest on an ethical framework that can identify fundamental, shareable principles to shape OSPs' conduct.

As OSPs' gatekeeping role impacts both users' access to information and the dynamics of the informational environment, any ethical framework that defines such principles should account for the rights of both users and the environment. Recalling the two LoAs adopted in the previous analysis, this ethical framework should endorse a LoA_{FOR}, that is a LoA that can identify principles and OSPs' responsibilities *for* the informational environment, fostering its flourishing and the wellbeing of the entities inhabiting it.

An ethical framework endorsing such an environmental approach has been proposed in Floridi (2013). An analysis of OSPs' responsibilities embracing Information Ethics has not yet been provided. However, some key aspects of this ethical framework—especially the concepts of 'care' and 'respect'; the flourishing of the environment as a function of its plurality and diversity; and ultimately the responsibility of human agents to care for the design and management of the informational environment so to ensure its wellbeing (Floridi and Taddeo 2014; Taddeo 2014) fit particularly well with the need to identify fundamental sharable ethical principles that may guide OSPs' conduct. Thus the previous analysis lays the ground for such a framework, the definition of which will be the focus of our future work.

References

Aceto, G., Botta, A., Pescapè, A., Feamster, N., Awan, M. F., Ahmad, T., et al. (2015). Monitoring internet censorship with UBICA. In M. Steiner, P. Barlet-Ros & O. Bonaventure (Eds.), *Traffic monitoring and analysis*, 143–57. Lecture Notes in Computer Science 9053. Springer International Publishing. http://link.springer.com/chapter/10.1007/978-3-319-17172-2_10

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on electronic commerce*, 21–29. EC'04. New York: ACM. doi:10.1145/988772.988777

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security Privacy, 3*(1), 26–33. doi:10.1109/MSP.2005.22

Albareda, L., Lozano, J. M., & Ysa, T. (2007). Public policies on corporate social responsibility: The role of governments in Europe. *Journal of Business Ethics, 74*(4), 391–407. doi:10.1007/s10551-007-9514-1

Anderson, M. (2008). The gaze of the perfect search engine: Google as an institution of dataveillance. In A. Spink & M. Zimmer (Eds.), *Web search: Multidisciplinary perspectives* (pp. 77–99). Berlin: Springer.

Anderson, G. (2012). *Just business*. London: Headline.

Arnold, D. G. (2010). Transnational corporations and the duty to respect basic human rights. *Business Ethics Quarterly, 20*(3), 371–399.

Bandura, A. (1999). Social cognitive theory: An agentic perspective. *Asian Journal of Social Psychology, 2*(1), 21–41. doi:10.1111/1467-839X.00024

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). doi:10.5210/fm.v11i9.1394

Barzilai-Nahon, K. (2008). Toward a theory of network gatekeeping: A framework for exploring information control. *Journal of the American Society for Information Science and Technology, 59*(9), 1493–1512. doi:10.1002/asi.20857

Baym, N. K. (2011). Social Networks 2.0. In M. Consalvo & C. Ess (Eds.), *The handbook of internet studies* (pp. 384–405). Wiley. http://onlinelibrary.wiley.com/doi/10.1002/9781444314861.ch18/summary

Besmer, A., Lipford, H. R., Shehab, M. & Cheek, G. (2009). Social applications: Exploring a more secure framework. In *Proceedings of the symposium on usable privacy and security* (*SOUPS*).

Black, J. (2001). Decentring regulation: Understanding the role of regulation and self regulation in a 'Post-Regulatory' world. *Current Legal Problems, 54*(1), 103–146.

Blowfield, M., & Murray, A. (2008). *Corporate responsibility: A critical introduction*. OUP Oxford: New York.

Blumenthal, M. S., & Clark, D. D. (2001). Rethinking the design of the Internet: The end to end arguments vs. the brave new world. *ACM Transactions on Internet Technology, 1*(1), 70–109.

Boca, P. (2014). *Formal methods: State of the art and new directions*. Berlin: Springer.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340–347.
Brenkert, G. G. (2009). Google, human rights, and moral compromise. *Journal of Business Ethics, 85*(4), 453–478. doi:10.1007/s10551-008-9783-3
Burk, D. L. (2011). Toward an epistemology of ISP secondary liability. In *SSRN scholarly paper ID 1920050*. Rochester: Social Science Research Network. http://papers.ssrn.com/abstract=1920050
Calhoun, C. J. (Ed.). (2002). *Dictionary of the social sciences*. New York: Oxford University Press.
Cate, F., Cullen, P. & Mayer-Schönberger, V. (2014). *Data protection principles for the 21st century, revising the 1980 OECD guidelines*. http://www.microsoft.com/en-us/download/details.aspx?id=41191
Caudill, E., & Murphy, P. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing, 19*(1), 7–19. doi:10.1509/jppm.19.1.7.16951
Cavoukian, A. (2014). *The unintended consequences of privacy paternalism*. Canadian Electronic Library. Canadian Public Policy Collection.
Cerf, V. G. (2011). First, do no harm. *Philosophy & Technology, 24*(4), 463–465. doi:10.1007/s13347-011-0056-1
Chen, S. (2009). Corporate responsibilities in internet-enabled social networks. *Journal of Business Ethics, 90*(4), 523–536. doi:10.1007/s10551-010-0604-0
Cragg, W. (2010). Business and human rights: A principle and value-based analysis. In G. G. Brenkert & T. L. Beauchamp (Eds.), *The oxford handbook of business ethics*. Oxford: Oxford University Press.
Crane, A., Matten, D., McWilliams, A., Moon, J. & Siegel, D. S. (Eds.). (2008). *The oxford handbook of corporate social responsibility* (1st ed.). Oxford University Press. http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199211593.001.0001/oxfordhb-9780199211593
Crawford, S. P. (2005). Shortness of vision: Regulatory ambition in the digital age. http://dash.harvard.edu/handle/1/12933354
Dann, G. E., & Haddow, N. (2007). Just doing business or doing just business: Google, Microsoft, Yahoo! and the business of censoring China's Internet. *Journal of Business Ethics, 79*(3), 219–234. doi:10.1007/s10551-007-9373-9
Diamond, L. (2010). Liberation technology. *Journal of Democracy, 21*(3), 69–83. doi:10.1353/jod.0.0190
Diaz, A. (2008). Through the Google goggles: Sociopolitical bias in search engine design. In A. Spink & M. Zimmer, *Web search* (pp. 11–34). Information Science and Knowledge Management 14. Berlin: Springer. http://link.springer.com/chapter/10.1007/978-3-540-75829-7_2
Diller, A. (1994). *Z: An introduction to formal methods* (2nd ed.). New York: Wiley.
Donaldson, T. (1992). *The ethics of international business*., The Ruffin Series in Business Ethnics New York: Oxford Univ. Press.
Donaldson, T., & Dunfee, T. W. (1999). *Ties that bind: A social contracts approach to business ethics*. Boston: Harvard Business School Press.
Edwards, L. (2011). *Role and responsibility of the internet intermediaries in the field of copyright and related rights*. *Report*. Geneva: WIPO. http://strathprints.strath.ac.uk/35492/
Elkin-Koren, N. (2001). Let the crawlers crawl: On virtual gatekeepers and the right to exclude indexing. *University of Dayton Law Review, 26*, 179–188.
Eriksson, J., & Giacomello, G. (2009). Who controls the internet? Beyond the obstinacy or obsolescence of the state. *International Studies Review, 11*(1), 205–230. doi:10.1111/j.1468-2486.2008.01841.x
Etzioni, A. (1999). *The limits of privacy*. New York: Basic Books.
Floridi, L. (2008). The method of levels of abstraction. *Minds and Machines, 18*(3), 303–329. doi:10.1007/s11023-008-9113-7
Floridi, L. (2013). *The ethics of information*. Oxford: Oxford University Press.
Floridi, L. (2015a). Free online services: Enabling, disenfranchising, disempowering. *Philosophy & Technology, 28*(2), 163–166. doi:10.1007/s13347-015-0200-4
Floridi, L. (2015b). Should you have the right to be forgotten on google? Nationally, yes. Globally, no. *New Perspectives Quarterly, 32*(2), 24–29. doi:10.1111/npqu.11510
Floridi, L., & Taddeo, M. (Eds.). (2014). *The ethics of information warfare*. New York: Springer.
Freeman, J. (1999). Private parties, public functions and the new administrative law. In *SSRN scholarly paper ID 165988*. Rochester: Social Science Research Network. http://papers.ssrn.com/abstract=165988
Friedmann, D. (2014). Sinking the safe harbour with the legal certainty of strict liability in sight. *Journal of Intellectual Property Law & Practice, 9*(2), 148–155. doi:10.1093/jiplp/jpt227

Gerry, F., & Berova, N. (2014). The rule of law online: Treating data like the sale of goods: Lessons for the internet from OECD and CISG and sacking google as the regulator. *Computer Law & Security Review, 30*(5), 465–481.

Goldman, E. (2006). Search engine bias and the demise of search engine utopianism. In *SSRN scholarly paper ID 893892*. Rochester: Social Science Research Network. http://papers.ssrn.com/abstract=893892

Granka, L. A. (2010). The politics of search: A decade retrospective. *The Information Society, 26*(5), 364–374. doi:10.1080/01972243.2010.511560

Hanel, P. (2006). Intellectual property rights business management practices: A survey of the literature. *Technovation, 26*(8), 895–931. doi:10.1016/j.technovation.2005.12.001

Hargittai, E. (2007). The social, political, economic, and cultural dimensions of search engines: An introduction. *Journal of Computer-Mediated Communication, 12*(3), 769–777. doi:10.1111/j.1083-6101.2007.00349.x

Heath, D., Allum, D., & Dunckley, L. (1994). *Introductory logic and formal methods*. Henley-on-Thames: Alfred Waller.

Helgesson, K. S., & Mörth, U. (Eds.). (2013). *The political role of corporate citizens: An interdisciplinary approach*., Palgrave studies in citizenship transitions series New York: Palgrave Macmillan.

Hildebrandt, M. (2013). Balance or trade-off? Online security technologies and fundamental rights. *Philosophy & Technology, 26*(4), 357–379. doi:10.1007/s13347-013-0104-0

Hinman, L. (2005). Esse est indicato in google: Ethical and political issues in search engines. *International Review of Information Ethics, 3*(6), 19–25.

Hinman, L. (2008). Searching ethics: The role of search engines in the construction and distribution of knowledge. In A. Spink & M. Zimmer (Eds.), *Web search* (pp. 67–76). Information Science and Knowledge Management 14. Berlin: Springer. http://link.springer.com/chapter/10.1007/978-3-540-75829-7_5

Hoare, C. A. R. (1972). Structured programming. In O. J. Dahl, E. W. Dijkstra, & C. A. R. Hoare (Eds.) (pp. 83–174). London: Academic Press Ltd. http://dl.acm.org/citation.cfm?id=1243380.1243382

Huberman, B. A. (2003). *The laws of the web: Patterns in the ecology of information*. London: MIT Press.

Hull, G., Lipford, H. R., & Latulipe, C. (2011). Contextual gaps: Privacy issues on facebook. *Ethics and Information Technology, 13*(4), 289–302. doi:10.1007/s10676-010-9224-8

Human Rights Council of the United Nations. (2012). *U.N. human rights council: First resolution on internet free speech*. http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403231_text

Introna, L. D., & Nissenbaum, H. (2006). Shaping the web: Why the politics of search engines matters. In *SSRN scholarly paper ID 222009*. Rochester: Social Science Research Network. http://papers.ssrn.com/abstract=222009

Jacky, J. (1997). *The way of Z: Practical programming with formal methods*. New York: Cambridge University Press.

Johnson, D. G. (2009). *Computer ethics* (4th ed.). Upper Saddle River: Pearson.

Jolls, C., & Sunstein, C. R. (2005). Debiasing through law. In *Working paper 11738*. National Bureau of Economic Research. http://www.nber.org/papers/w11738

Karp, D. J. (2009). Transnational corporations in 'bad States': Human rights duties, legitimate authority and the rule of law in international political theory. *International Theory, 1*(01), 87. doi:10.1017/S1752971909000074

Kerr, I. (2002). Internet users dependence and the duty of loyalty. In T. Mendina & B. Rockenbach (Eds.), *Ethics and electronic information* (pp. 166–176). North Carolina: McFarland Press.

Kiss, A., & Szőke G. L. (2015). Evolution or revolution? Steps forward to a new generation of data protection regulation. In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 311–31). Law, Governance and Technology Series 20. Springer Netherlands. http://link.springer.com/chapter/10.1007/978-94-017-9385-8_13

Laidlaw, E. (2008). Private power, public interest: An examination of search engine accountability. *International Journal of Law and Information Technology, 17*(1), 113–145. doi:10.1093/ijlit/ean018

Laidlaw, E. (2010). A framework for identifying internet information gatekeepers. *International Review of Law, Computers & Technology, 24*(3), 263–276. doi:10.1080/13600869.2010.522334

Lampinen, A., Lehtinen, V., Lehmuskallio, A., & Tamminen, S. (2011). We'Re in it together: Interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI conference on human factors in computing systems*, 3217–26. CHI'11. New York: ACM. doi:10.1145/1978942.1979420

Lanier, J. (201)1. *You are not a gadget: A manifesto* (Reprint edition). New York: Vintage

Lessig, L. (1999). *Code: And other laws of cyberspace*. New York: Basic Books.
Lessig, L. (2007). In support of network neutrality. *I/S: A Journal of Law and Policy for Information Society, 3*(1), 185–196.
Lev-On, A. (2009). The democratizing effects of search engine use: On chance exposures and organizational hubs. In *SSRN scholarly paper ID 1481901*. Rochester: Social Science Research Network. http://papers.ssrn.com/abstract=1481901
Lev-On, A., & Manin, B. (2009). Happy accidents: Deliberation and online exposure to opposing views. In: T. Davies & S. P. Gangadharan (Eds.), *Online deliberation: Design, research and practice*. Stanford: CSLI Publications.
Lewandowski, D. (2011). The influence of commercial intent of search results on their perceived relevance. Preprint. February 8. http://eprints.rclis.org/17232/
Lewin, K. (1947). Frontiers in group dynamics. *Human Relations, 1*(2), 143–153.
Madden, M. (2012). Privacy management on social media sites. *Pew Internet Report*.
Madelin, R. (2011). The evolving social responsibilities of internet corporate actors: Pointers past and present. *Philosophy & Technology, 24*(4), 455–461. doi:10.1007/s13347-011-0049-0
Matten, D., & Crane, A. (2005). Corporate citizenship: Toward an extended theoretical conceptualization. *Academy of Management Review, 30*(1), 166–179.
Mayer-Schönberger, V. (2011). *Delete: The virtue of forgetting in the digital age*. Princeton: Princeton University Press.
McQuail, D. (1992). *Media performance: Mass communication and the public interest*. Newbury Park: Sage Publications.
Metoyer-Duran, C. (1993). Information gatekeepers. *Annual Review of Information Science and Technology (ARIST), 28*, 111–150.
Nagenborg, M. (2005). The ethics of search engines (special issue). *International Review of Information Ethics* 3.
Negroponte, N. (1996). *Being digital*. New edition edition. Rydalmere: Coronet Books.
Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford: Stanford Law Books.
Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126. doi:10.1111/j.1745-6606.2006.00070.x
O'Hara, K. (2010). Intimacy 2.0: Privacy rights and privacy responsibilities on the World Wide Web. In J. Zittrain, J. Domingue, & N. Benn (Eds.). http://eprints.soton.ac.uk/268760/
OECD. (2013). *OECD guidelines on the protection of privacy and transborder flows of personal data*. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
Okoye, A. (2009). Theorising corporate social responsibility as an essentially contested concept: Is a definition necessary? *Journal of Business Ethics, 89*(4), 613–627. doi:10.1007/s10551-008-0021-9
Pagallo, U. (2011). ISPs & rowdy web sites before the law: Should we change today's safe harbour clauses? *Philosophy & Technology, 24*(4), 419–436. doi:10.1007/s13347-011-0031-x
Palazzo, G., & Scherer, A. G. (2006). Corporate legitimacy as deliberation: A communicative framework. *Journal of Business Ethics, 66*(1), 71–88. doi:10.1007/s10551-006-9044-2
Pandey, S, Roy, S., Olston, C., Cho, J. & Chakrabarti, S. (2005). Shuffling a stacked deck: The case for partially randomized ranking of search engine results. In *Proceedings of 31st international conference on very large databases* (*VLDB*) (pp. 781–92).
Pariser, E. (2012). *The filter bubble: What the internet is hiding from you*. London: Penguin.
Pasquale, F. A. (2006). Rankings, reductionism, and responsibility. In *SSRN scholarly paper ID 888327*. Rochester: Social Science Research Network. http://papers.ssrn.com/abstract=888327
Qi, M., & Edgar-Nevill, D. (2011). Social networking searching and privacy issues. *Information Security Technical Report*. doi:10.1016/j.istr.2011.09.005
Reding, V. (2012). *The EU data protection reform 2012: Making Europe the standard setter for modern data protection rules in the digital age*. European Commission. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF
Reger, C. M. (2004). Let's swap copyright for Code: The computer software disclosure dichotomy. *Loyola of Los Angeles Entertainment Law Review, 24*, 215.
Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online, 64*, 88.
Rosen, J. (2015). Protecting privacy on the internet is the user's responsibility. *Philly-Archives*. http://articles.philly.com/2012-03-05/news/31124410_1_new-privacy-policy-facebook-search-terms

Santoro, M. A. (1998). Engagement with integrity: What we should expect multinational firms to do about human rights in China. *Business and the Contemporary World*, *10*(1), 25–54.
Schahczenski, C. (2008). Net neutrality, computing and social change. *ACM SIGCAS Computers and Society, 38*(2), 27.
Scherer, A. G., & Palazzo, G. (2006). Toward a political conception of corporate responsibility-business and society seen from a habermasian perspective. In *SSRN scholarly paper ID 952013*. Rochester: Social Science Research Network. http://papers.ssrn.com/abstract=952013
Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology, 16*(2), 171–182. doi:10.1007/s10676-014-9343-8
Schwartz, P. (1999). Privacy and democracy in cyberspace. *Vanderbilt Law Review, 52*(1999), 1607.
Semitsu, J. P. (2011). From facebook to mug shot: How the dearth of social networking privacy rights revolutionized online government surveillance. In *SSRN scholarly paper ID 1782267*. Rochester: Social Science Research Network. http://papers.ssrn.com/abstract=1782267
Shapiro, A. L. (2000). *The control revolution: How the internet is putting individuals in charge and changing the world we know* (2nd Printing ed.). New York: PublicAffairs.
Smith, H. Jeff, Dinev, T., & Heng, X. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1016.
Solove, D. J. (2008). Understanding privacy. In *SSRN scholarly paper ID 1127888*. Rochester: Social Science Research Network. http://papers.ssrn.com/abstract=1127888
Spinello, R. A. (2011). Privacy and social networking technology. *International Review of Information Ethics, 16*, 12.
Spink, A., & Zimmer, M. (2008). *Web search* (Vol. 14). Information Science and Knowledge Management. Berlin: Springer.
Sunstein, C. R. (2001). *Republic.com*. With a new afterword by the author edition. Princeton: Princeton University Press.
Taddeo, M. (2010). Modelling trust in artificial agents, a first step toward the analysis of e-trust. *Minds and Machines, 20*(2), 243–257. doi:10.1007/s11023-010-9201-3
Taddeo, M. (2013). Cyber security and individual rights, striking the right balance. *Philosophy & Technology, 26*(4), 353–356. doi:10.1007/s13347-013-0140-9
Taddeo, M. (2014). The struggle between liberties and authorities in the information age. *Science and Engineering Ethics*, 1–14. doi:10.1007/s11948-014-9586-0
Tavani, H. (2014). Search engines and ethics. In E. N. Zalta (Ed.), *The stanford encyclopedia of philosophy*. http://plato.stanford.edu/archives/spr2014/entries/ethics-search/
Tavani, H., & Grodzinsky, F. S. (2002). Cyberstalking, personal privacy, and moral responsibility. *Ethics and Information Technology, 4*(2), 123–132. doi:10.1023/A:1019927824326
Tavani, H., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *SIGCAS Compututers and Society, 31*(1), 6–11. doi:10.1145/572277.572278
Toffler, A., Heidi, T., & Newt, G. (1995). *Creating a new civilization: The politics of the third wave* (1st ed.). Kansas City: Turner Publishing.
Turilli, M., Vaccaro, A., & Taddeo, M. (2010). The case of online trust. *Knowledge, Technology & Policy, 23*(3–4), 333–345. doi:10.1007/s12130-010-9117-5
Turilli, M., Vaccaro, A., & Taddeo, M. (2012). Internet neutrality: Ethical issues in the internet environment. *Philosophy & Technology, 25*, 133–151.
Van Couvering, E. (2007). Is relevance relevant? Market, science, and war: Discourses of search engine quality. *Journal of Computer-Mediated Communication, 12*(3), 866–887. doi:10.1111/j.1083-6101.2007.00354.x
Vedder, A. (2001). Accountability of internet access and service providers—Strict liability entering ethics? *Ethics and Information Technology, 3*(1), 67–74. doi:10.1023/A:1011492109277
Wang, N., Xu, H., & Grossklags, J. (2011). Third-party apps on facebook: Privacy and the illusion of control. In *Proceedings of the 5th ACM symposium on computer human interaction for management of information technology*, 4:1–4:10. CHIMIT'11. New York: ACM. doi:10.1145/2076444.2076448
Weckert, J. (2005). Trust in cyberspace. In R. J. Cavalier (Ed.), *The impact of the internet on our moral lives* (pp. 95–120). Albany: University of New York Press.
Wettstein, F. (2012). Silence as complicity: Elements of a corporate duty to speak out against the violation of human rights. *Business Ethics Quarterly, 22*(01), 37–61. doi:10.1017/S1052150X00000063

Wolf, M. J., Miller, K. W., & Grodzinsky, F. S. (2009). On the meaning of free software. *Ethics and Information Technology, 11*(4), 279–286. doi:10.1007/s10676-009-9207-9

Wolf, D., Ralf, K. W., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in facebook. *Computers in Human Behavior, 35*, 444–454. doi:10.1016/j.chb.2014.03.010

World Economic Forum. (2012). Unlocking the economic value of personal data balancing growth and protection. http://www3.weforum.org/docs/WEF_IT_UnlockingValueData_BalancingGrowthProtection_SessionSummary.pdf

Xu, H. (2012). Reframing privacy 2.0 in online social networks. *University of Pennsylvania Journal of Constitutional Law, 14*(4), 1077.

Ziniti, C. (2008). Optimal liability system for online service providers: How Zeran v. America online got it right and web 2.0 proves it. *Berkeley Technology Law Journal, 23*, 583.