Law, Governance and Technology Series 31

Mariarosaria Taddeo
Luciano Floridi *Editors*

The Responsibilities of Online Service Providers

Springer

Law, Governance and Technology Series

Volume 31

The *Law, Governance and Technology Series* is intended to attract manuscripts arising from an interdisciplinary approach in law, artificial intelligence and information technologies. The idea is to bridge the gap between research in IT law and IT-applications for lawyers developing a unifying techno-legal perspective. The series will welcome proposals that have a fairly specific focus on problems or projects that will lead to innovative research charting the course for new interdisciplinary developments in law, legal theory, and law and society research as well as in computer technologies, artificial intelligence and cognitive sciences. In broad strokes, manuscripts for this series may be mainly located in the fields of the Internet law (data protection, intellectual property, Internet rights, etc.), Computational models of the legal contents and legal reasoning, Legal Information Retrieval, Electronic Data Discovery, Collaborative Tools (e.g. Online Dispute Resolution platforms), Metadata and XML Technologies (for Semantic Web Services), Technologies in Courtrooms and Judicial Offices (E-Court), Technologies for Governments and Administrations (E-Government), Legal Multimedia, and Legal Electronic Institutions (Multi-Agent Systems and Artificial Societies).

More information about this series at http://www.springer.com/series/8808

Mariarosaria Taddeo • Luciano Floridi
Editors

The Responsibilities of Online Service Providers

Springer

Editors

Mariarosaria Taddeo
Oxford Internet Institute
University of Oxford
Oxford, UK

Alan Turing Institute
London, UK

Luciano Floridi
Oxford Internet Institute
University of Oxford
Oxford, UK

Alan Turing Institute
London, UK

ISSN 2352-1902 ISSN 2352-1910 (electronic)
Law, Governance and Technology Series
ISBN 978-3-319-47851-7 ISBN 978-3-319-47852-4 (eBook)
DOI 10.1007/978-3-319-47852-4

Library of Congress Control Number: 2017931074

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Part III Users' Rights & International Regulations

Part IV Commentaries

About the Editors

Mariarosaria Taddeo works at the Oxford Internet Institute, University of Oxford and Faculty Fellow at the Alan Turing Institute. Her recent work focuses mainly on the ethical analysis of cyber security practices and information conflicts. Her area of expertise is Information and Computer Ethics, although she has worked on issues concerning Philosophy of Information, Epistemology, and Philosophy of AI. She published several papers focusing on online trust, cyber security and cyber warfare and guest-edited a number of special issues of peer-reviewed international journals: Ethics and Information Technology, Knowledge, Technology and Policy, Philosophy & Technology. She also edited (with L. Floridi) a volume on 'The Ethics of Information Warfare' (Springer 2014) and is currently writing a book on 'The Ethics of Cyber Conflicts' under contract for Routledge. Dr. Taddeo is the 2010 recipient of the Simon Award for Outstanding Research in Computing and Philosophy and of the 2013 World Technology Award for Ethics. She serves editor-in-chief of Minds & Machines, in the executive editorial board of Philosophy & Technology. Since 2016, Dr. Taddeo is Global Future Council Fellow for the Council on the Future of Cybersecurity of the World Economic Forum.

Luciano Floridi is professor of philosophy and ethics of information at the University of Oxford and director of research of the Oxford Internet Institute. His most recent book is *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (2014 and 2016). He is a member of the EU's Ethics Advisory Group on ethical dimensions of data protection and of Google's advisory board on "the right to be forgotten" and chairman of the Ethics Advisory Board of the European Medical Information Framework. Among his recognitions, he has been elected Fernand Braudel senior fellow by the European University Institute, was awarded the Cátedras de Excelencia Prize by the University Carlos III of Madrid, and was the UNESCO chair in information and computer ethics and Gauss professor of the Academy of Sciences in Göttingen. He is a recipient of the MEA's J. Ong Award, the APA's Barwise Prize, the IACAP's Covey Award, and the INSEIT's Weizenbaum Award. He is a fellow of the AISB, the BCS, and the Académie Internationale de Philosophie des Sciences.

Chapter 1
New Civic Responsibilities for Online Service Providers

Mariarosaria Taddeo and Luciano Floridi

Online Service Providers (OSPs)—such as AOL, Facebook, Google, Microsoft, and Twitter—are increasingly expected to act as good citizens, by aligning their goals with the needs of societies, supporting the rights of their users (Madelin 2011; Taddeo and Floridi 2015), and performing their tasks according to "principles of efficiency, justice, fairness, and respect of current social and cultural values" (McQuail 1992, 47). These expectations raise questions as to what kind of responsibilities OSPs should bear, and which ethical principles should guide their actions.

Addressing these questions is a crucial step to understand and shape the role of OSPs in mature information societies (Floridi 2016). Without a clear understanding of their responsibilities, we risk ascribing to OSPs a role that is either too powerful or too little independent. The FBI vs. Apple case,[1] Google's and Yahoo!'s experiences in China,[2] or the involvement of OSPs within the NSA's PRISM program[3] offer good examples of the case in point. However, defining OSPs' responsibilities is challenging. Three aspects are particularly problematic: disentangling the implications of OSPs' gatekeeping role in information societies; defining fundamental principles to guide OSPs' conduct; and contextualising OSPs' role within the broader changes brought about by the information revolution.

The notion of 'gatekeepers' identifies those agents who have a central role in the management of resources and infrastructures that are crucial for societies (Lewin 1947). In our societies, OSPs are *information* gatekeepers (Calhoun 2002), as they control access to and flows of data and information (Shapiro 2000; Hinman 2005; Laidlaw 2008). As such, they exercise a regulatory function (Metoyer-Duran 1993), which entails moral responsibilities toward the public good. As Shapiro put it

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

[1] https://en.wikipedia.org/wiki/FBI–Apple_encryption_dispute

[2] http://business.time.com/2014/01/08/are-google-yahoo-and-microsoft-living-up-to-their-promises-in-china/

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

M. Taddeo (✉) • L. Floridi
Oxford Internet Institute, University of Oxford, Oxford, UK

Alan Turing Institute, London, UK
e-mail: mariarosaria.taddeo@oii.ox.ac.uk

M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*,
Law, Governance and Technology Series 31, DOI 10.1007/978-3-319-47852-4_1

While there is a general consensus on OSPs' gatekeeping role and on their ability to influence the development of information societies, there is much less agreement on whether, as corporate agents, OSPs bear any responsibility toward the public good (Freeman 1999; Black 2001; Taddeo and Floridi 2015). As a result, the civic responsibilities of OSPs are often discharged *via* policies and practices unilaterally defined by OSPs themselves.

Things become more complicated once we consider the international and inevitably multicultural contexts in which OSPs operate, the transnational nature of their business, alongside the interdependency of the services that they offer in different regions of the world. In this context, the definition of the responsibilities of OSPs will be effective only insofar as it will rest on an ethical framework able to reconcile the different views and stakeholders' interests that they face.

Human rights have a central role in this debate, insofar as they identify fundamental universal principles, some of which expressly address Internet governance (Wettstein 2012b; Lucchi 2013). For example, a report[4] released by the UN in 2011stressed that

> [g]iven the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States.

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.[5] However, both the Universal Declaration of Human Rights and the Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet[12] mainly address state actors, making problematic the expectation that OSPs should be held responsible for respecting and fostering human rights (Karp 2009). This problem is not entirely new. The scope of human rights and the responsibilities that they pose to transnational corporations have already been analysed in the Declaration of Human Duties and Responsibilities (the so-called Valencia Declaration). The Declaration stresses the moral duties and legal responsibilities of all 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 human rights in the preamble of the UN Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises.

Given OSPs' central role in shaping the informational environment and the societies depending on it, it is increasingly less acceptable to maintain that, as private companies, OSPs are only responsible to their employees and shareholders, and are

[4] http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

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

not bounded by human rights regulation (Chen 2009; Taddeo and Floridi 2015; Cath and Floridi 2016; Laidlaw Forthcoming). This is a point highlighted, for example, in the latest report of the Special Rapporteur on freedom of expression to the Human Rights Council, David Kaye, who stressed that

> Among the most important steps that private actors should take is the development and implementation of transparent human rights assessment procedures. They should develop and implement policies that take into account their potential impact on human rights.[6]

At the same time, however, it is problematic to ascribe to OSPs full responsibility for fostering and respecting human rights, and for deciding the circumstances in which these apply. For this prompts a privatization of the judging power and poses issues of transparency and accountability (Gerry and Berova 2014). Consider, for example, OSPs acting as both the "judge and the jury"[7] with respect to the decision of the European Court of Justice on the right to be forgotten (Rosen 2012; Floridi 2015). To this end, it is crucial to separate the responsibilities of OSPs from the duties and authority of the state.

Guidance on this matter has been provided by the Ruggie's framework.[8] The framework proposes a clear-cut distinction between the role of states and that of transnational corporations with respect to human rights (Wettstein 2012a). The distinction rests on three pillars: the duty of the state to *protect* against human rights abuses by third parties, including business; the corporate responsibility to *respect* human rights; and the responsibility of both states and corporates to provide victims with access to effective *remedy*, both judicial and non-judicial.

While the Ruggie's framework offers a valid tool to identify the responsibilities of transnational corporations, the proposed distinction between states' duties and corporates' responsibilities proves to be problematic when considering specifically the case of OSPs. Their crucial role in information societies, alongside their leading role in steering the information revolution and, hence, in shaping the informational environment make them political agents able to influence national politics and international relations (Broeders and Taylor forthcoming). As such, they differ quite radically from other transnational corporations and bear a wider set of responsibilities than other corporate agents (Scherer and Palazzo 2011). Broders and Taylor argue that, as political agents, OSPs should bear corporate *political* responsibilities:

> OSPs exercise power over their users and are a counter power to state power in all corners of the world. […] they are also political actors who merit serious diplomatic attention owing to their vital role in digital life, […] (Broeders and Taylor forthcoming).

The Ruggie's framework only partially addresses OSPs' political role and offers little insight to identify states' duties in cyberspace. Insofar as the framework rests on the Westphalian model of sovereign states, it struggles to address new forms of

[6] http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Privatesectorinthedigitalage.aspx

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

[8] http://198.170.85.29/Ruggie-protect-respect-remedy-framework.pdf

political agents—like the EU and the UN—or NGOs (Nye 2004). At the same time, the model is challenged when considering sovereign states' authority in cyberspace, where it is problematic to draw national boundaries, and state's territoriality and sovereignty are difficult to define (Krasner 2001).

The limitations of the Ruggie's framework point to the third set of problems concerning the definition of OSPs' civic responsibilities, namely the understanding of the conceptual and moral changes (Floridi 2014a, b; Taddeo and Buchanan 2015) brought about by new phenomena such as, for example, Big Data analytics (Floridi 2012; Mittelstadt and Floridi 2015), individual and group privacy (Floridi 2014a, b), online trust (Taddeo 2010; Taddeo and Floridi 2011), cyber security and surveillance (Taddeo 2013; Taddeo 2014b), and cyber conflicts (Taddeo 2012; Taddeo 2014a; Floridi and Taddeo 2014). These changes concern the redefinition of crucial concepts, like those of political power and authority, as well as the distinction between real and virtual and the understanding of good and evil, and of the values on which present and future information societies rely.

The civic responsibilities of OSPs cannot be defined without considering these conceptual changes and without a foresight analysis of the future of information societies, toward which OSPs play a decisive role. In (Taddeo and Floridi 2015), we argued that the notion of information gatekeepers, the human rights framework, and the concepts of *respect* and *care for* the informational environment (Floridi 2013a) offer key milestones for an ethical framework able to identify and define both the civic responsibilities of OSPs and the right ethical infrastructure, i.e. the *infraethics (*Floridi 2013b), able to facilitate the discharging of such responsibilities. This requires identifying those

> expectations, attitudes, and practices that *can* facilitate and promote morally good decision and actions (Floridi 2013b, 738).

In the case of OSPs, the right infraethics encompasses trust, privacy, and transparency, as well as openness and pluralism.

It is clear that the definition of OSPs' responsibilities and of the infraethics supporting them will increasing shape the informational environment and future information societies (Floridi 2011; Cath and Floridi 2016). For this reason *ad hoc* approaches, tackling OSPs' responsibilities as they emerge, will be insufficient in the medium- and long-term, for they lack a meaningful reflection on current changes and any insight on future ones. Both can only be achieved by coordinating expertise and theorising to understand the values that will continue shaping our societies, the different stakeholders' views, alongside the role of OSPs and of other key agents in designing the informational environment.

This volume provides a step in this direction, by collecting eighteen contributions addressing the issue of OSPs' responsibilities from different angles. Each contribution is either invited or a paper presented during the workshop "*Understanding the Responsibilities of Online Service Providers in Information Societies*", held in 2015 at the Oxford Internet Institute, University of Oxford. The goal is to offer a multidisciplinary collection of essays spanning from ethics and corporate social responsibilities to policy and legal analyses of OSPs civic responsibilities. The volume is divided into three parts, focusing on ‘Responsibilities & Liabilities’, ‘Business Ethics & Policies’, and ‘Users’ Rights & International Regulations’ respectively.

Chapter two—*The moral responsibilities of online service providers*—opens the first part of the book, with a reprinted version of a paper appeared in 2015 (Taddeo and Floridi 2015). It analyses the main contributions to the debate on the moral responsibilities of OSPs. By endorsing the method of the levels of abstraction (LoAs) (Floridi 2008), it first focuses on 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. The chapter then delves into the moral responsibilities ascribed to OSPs *on* the web (LoA_{ON}) describing existing legal regulations of access to users’ data. The analysis highlights two main results. First, OSPs’ public role—especially their gatekeeping function, their corporate social responsibilities, and their role in implementing and fostering human rights—has 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.

The analysis of OSPs responsibilities in the web continues in the third chapter—*The immunity of internet intermediaries reconsidered?*—which focuses on the role of OSPs in the digital world. The goals of this contribution are to identify the role of new power players in the digital world and to analyse the boundaries between immunity and liability of Internet intermediaries. Specifically, this contribution addresses questions such as: will OSPs become *quasi judges* controlling every Internet activity? Are they entitled to defend the rights of the users and, more in general, the legitimacy in cyberspace? Which principles and policies should be adopted in order to foster an ethos of compliance and social responsibility for these new gatekeepers?

Chapter four—*Is Google responsible for providing fair and unbiased results?*—focuses on the responsibility of search engines in general, and Google in particular, for providing unbiased search results. The chapter identifies areas of potential responsibilities of search engines by endorsing two approaches, one technical and the other societal. The technical approach considers the impact of decisions made at the design stage on users’ search results. The societal approach informs discussion on the impact that biased search engines may have for information and knowledge acquisition in society.

Chapter five—*Speaking truth to/as victims, a jurisprudential analysis of data breach notification laws*—analyses the duty that OSPs have to inform customers when the company suspects security breaches and unauthorised access to customer data. This chapter focuses on data breach notification duties from a jurisprudential perspective and considers what duties can legitimately be attributed to victims of crime in a democratic society. It then applies this analysis to OSPs and their duty to inform either their customers or a state agency about data breaches.

Chapter six—*Did the Romans get it right? What Delfi, Google, eBay, and UPC TeleKabel Wien have in common*—concludes the first part of the volume by providing a description of the legal principles set out in recent landmark cases of both the EU Court of Justice in Luxembourg (CJEU) and the European Court of Human Rights (ECHR), including the Google France, Google Spain/Costeja, UPC TeleKabel Wien and Delfi cases. It examines the legal grounds and arguments put forward by the respective courts in order to judge OSPs' responsibilities.

The second part of the book collects analyses focusing on business ethics and corporate social responsibilities. Chapter seven—*Responsibilities of OSPs from a business ethics point of view*—opens this part by focusing on a central aspect of the business ethics debate, i.e. the balance between OSPs' responsibilities and their ability to be competitive in the market. This chapter argues, first, that the analysis of OSPs' business responsibilities should rest less on purely individual concepts of responsibility and more on the concepts of group agency; and, second, that there are ways of ascribing responsibility to companies compatible with competition, as the debate on corporate social responsibilities (CSR) shows.

The analysis on OSPs' CSR continues in chapter eight—*Myth or promise? The corporate social responsibilities of online service providers for human rights*. The chapter analyses a number of CSR frameworks shaping OSPs' conduct. In particular, it concentrates on the UN Guiding Principles and on the Global Network Initiative, one of the leading multi-stakeholder initiatives guiding CSR for technology companies. The goal is to address OSPs' accountability with respect to human rights. In doing so, the chapter focuses on key issues such the relevance of CSR frameworks for protecting human rights online.

Chapter nine-*Online Service Providers—a new and unique species of the firm?*—draws on cross-disciplinary literature from economic theory, international business theory, economic geography, and information technology, in order to analyse whether OSPs differ from other transnational corporations and whether this entails different CSRs. The chapter concludes that, albeit OSPs differ from other transnational corporations, such difference are not wide enough to consider OSPs a unique kind of firm. The analysis then focuses on the non-monetary relationship between OSPs and their end-users, and on the societal impact that this could have, especially in developing countries.

Chapter ten—*Online service providers as human rights arbiters*—continues the analysis of fair policies for OSPs and of their responsibilities with respect to human rights. The chapter focuses on case-studies of EU regulation such as the E-commerce directive, to assess whether and to what extent measures of blocking, filtering, and content removal interfere with the human rights standards related to freedom of expression and freedom of information. The chapter concludes that OSPs' self-defined guidelines are insufficient to counter the human rights challenges.

Chapter eleven—*Licensing of user-generated content: why less is more*—delves into the responsibilities of OSPs with respect to users-generated content that is subject to licensing clauses found in terms of service agreements. The chapter argues that contractual ambiguity existing in OSPs' terms of service agreements negatively affects users and OSPs alike.

The third part of the book is dedicated to 'Users' rights & international regulations' and begins with chapter twelve—*Online service providers' liability, copyright infringement, and freedom of expression. Could Europe learn from Canada?* This contribution analyses recent interpretations of the Dir. 2000/31, which have lifted the bar on providers' duties and highlights their impact on OSPs business and, most important, on freedom of expression. The chapter then focuses on the Canadian regulation, which is based on the so-called 'notice and action' principle, and suggests it offers a suitable framework for the regulation of OSPs' liabilities in Europe.

Chapter thirteen—*Non-financial disclosures in the tech sector: furthering the trend*—focuses on transparency and analyses the different ways through which corporate non-financial disclosure mechanisms can contribute to developing an ethical framework for OSPs. The chapter discusses three areas where transparency makes an impact on ethical standards for OSPs: corporate reporting on interaction with governments on privacy and free expression issues; disclosures of staff demographics; and sharing of information on digital security topics, including encryption and breach. Finally, it assesses the ways through which transparency mechanisms, and their consistent implementation, could help OSPs realize their new civic responsibilities.

Chapter fourteen—*Should we treat Big Data as a public good?*—discusses Big Data and the responsibilities of OSPs to ensure that the user-generated data continue to improve individual well-being, innovation, and sustainable development. To this end the chapter maintains that Big Data should be considered a public good and that platforms for public and private partnerships in managing Big Data should be in place.

Chapter fifteen—*Internet intermediaries as responsible actors? Why it is time to rethink the e-Commerce Directive as well*—questions the suitability of the e-Commerce Directive. The purpose of this chapter is twofold. It aims to show that there is a need to review Articles 12 to 15 of the e-Commerce Directive; and that the very rationale linking Articles 12 to 14 of the e-Commerce Directive is ill-suited to address the complexity and diversity of OSPs' activities.

Chapter sixteen—*Towards fostering compliance by design, drawing designers into the regulatory frame*—begins by considering the extent to which EU General Data Protection Regulations would redefine the governance of personal data in a series of key ways and focuses, in particular, on the 'by design and by data protection'. It argues that this notion shifts the responsibility away from the user and explicitly invokes the role of the designer within the regulatory frame. The chapter then describes *ideation cards* as a suitable method to foster cross-disciplinary collaborations. It maintains that, whilst such cards will not necessarily create experts in data protection, they have the potential to sensitise designers to existing regulation.

Three commentaries conclude the volume. The first one—*Does great power come with great responsibility? The need to talk about Corporate Political Responsibility*—analyses the role of OSPs in contemporary societies and argues that OSPs act as political agents, with a relevant role in both national politics and international relations. Such a role requires extending the scope of the CSR that OSPs bear in two ways:

> […] more serious mechanisms for accountability and (b) a recognition of the political role of corporations (Broeders and Taylor forthcoming).

The second commentary—*The Economic Impact of Online Intermediaries* —focuses on the role of Internet intermediaries to drive economic, social, and political development and considers whether the consolidation of OSPs' economic power impacted conventional business trade models and changed firm-level competition. It concludes that, while OSPs have provided technologically superior market entrants, they have not yet disrupted supply-chains, with the exception of software, publishing, and professional services sectors, in which online intermediaries have provided tangible productivity gains.

The third commentary— *Online Service Providers and ethical disclosure in sales*—addresses the need to develop business norms for the commodification of user information by OSPs. This contribution maintains that in considering the responsibilities of OSPs, referring to business norms, rather than interpersonal moral norms, leads to draw ethical conclusions with clear normative force.

References

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.

Broeders, D., & Taylor, L. (Forthcoming). Does great power come with great responsibility? The need to talk about corporate political responsibility. In M. Taddeo & L. Floridi (Ed.), *Law, governance and technology series*. Berlin/Heidelberg/New York/London: Springer.

Calhoun, C. J. (Ed.). (2002). *Dictionary of the social sciences*. New York: Oxford University Press.

Cath, C., & Florid, L. (2016, May). The design of the internet's architecture by the Internet Engineering Task Force (IETF) and Human Rights. *Science and Engineering Ethics*.

Chen, S. (2009). Corporate responsibilities in internet-enabled social networks. *Journal of Business Ethics, 90*(4), 523–536.

Floridi, L. (2008). The method of levels of abstraction. *Minds and Machines, 18*(3), 303–329.

Floridi, L. (2011). A defence of constructionism: Philosophy as conceptual engineering. *Metaphilosophy, 42*(3), 282–304.

Floridi, L. (2012). Big data and their epistemological challenge. *Philosophy & Technology, 25*(4), 435–437.

Floridi, L. (2013a). *The ethics of information*. Oxford: Oxford University Press.

Floridi, L. (2013b). Distributed morality in an information society. *Science and Engineering Ethics, 19*(3), 727–743.

Floridi, L. (2014a). *The fourth revolution, how the infosphere is reshaping human reality*. Oxford: Oxford University Press.

Floridi, L. (2014b). Open data, data protection, and group privacy. *Philosophy & Technology, 27*(1), 1–3.

Floridi, L. (2015). Should you have the right to be forgotten on google? Nationally, Yes. globally, No. *New Perspectives Quarterly, 32*(2), 24–29.

Floridi, L. (2016). Mature information societies—A matter of expectations. *Philosophy & Technology, 29*(1), 1–4.

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*, *SSRN Scholarly Paper ID 165988*. Rochester: Social Science Research Network.

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.

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

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

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.

Krasner, S. D. (2001). Rethinking the sovereign state model. *Review of International Studies, 27*(05).

Laidlaw, E. (Forthcoming). Myth or promise? The corporate social responsibilities of online service providers for human rights. In M. Taddeo & L. Floridi (Eds.), *The responsibilities of online service providers* Law, governance and technology series. Berlin/Heidelberg/New York/London: Springer.

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

Lewin, K. (1947). Frontiers in group dynamics. Human Relations *1*(2), 143–153.

Lucchi, N. (2013). Internet content governance and human rights. *Vanderbilt Journal of Entertainment and Technology Law, 16*, 809.

Madelin, R. (2011). The evolving social responsibilities of internet corporate actors: Pointers past and present. *Philosophy & Technology, 24*(4), 455–461.

McQuail, D. (1992). *Media performance: Mass communication and the public interest*. London/Newbury Park: Sage Publications.

Metoyer-Duran, C. (1993). Information gatekeepers. *Annual Review of Information Science and Technology (ARIST), 28*, 111–150.

Mittelstadt, B. D., & Floridi, L. (2015). The ethics of big data: Current and foreseeable issues in biomedical contexts. *Science and Engineering Ethics*, May.

Nye, J. S. (2004). *Soft power: The means to success in world politics* (1st ed.). New York: Public Affairs.

Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online, 64*, 88.

Scherer, A. G., & Palazzo, G. (2011). The new political role of business in a globalized world: A review of a new perspective on CSR and its implications for the firm, governance, and democracy. *Journal of Management Studies, 48*(4), 899–931.

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: Public Affairs.

Taddeo, M. (2010). Modelling trust in artificial agents, A first step toward the analysis of E-trust. *Minds and Machines, 20*(2), 243–257.

Taddeo, M. (2012). Information warfare: A philosophical perspective. *Philosophy and Technology, 25*(1), 105–120.

Taddeo, M. (2013). Cyber security and individual rights, striking the right balance. *Philosophy & Technology, 26*(4), 353–356.

Taddeo, M. (2014a). Just information warfare. *Topoi*, April, 1–12.

Taddeo, M. (2014b). The struggle between liberties and authorities in the information age. *Science and Engineering Ethics*, September, 1–14.

Taddeo, M., & Buchanan, E. (2015). Information societies, ethical enquiries. *Philosophy & Technology, 28*(1), 5–10.

Taddeo, M., & Floridi, L. (2011). The case for E-trust. *Ethics and Information Technology, 13*(1), 1–3.

Taddeo, M., & Floridi, L. (2015). The debate on the moral responsibilities of online service providers. *Science and Engineering Ethics*.

Wettstein, F. (2012a). CSR and the debate on business and human rights: Bridging the great divide. *Business Ethics Quarterly, 22*(4), 739–770.

Wettstein, F. (2012b). Silence as complicity: Elements of a corporate duty to speak out against the violation of human rights. *Business Ethics Quarterly, 22*(01), 37–61.

Part I
Responsibilities and Liabilities

Chapter 2
The Moral Responsibilities of Online Service Providers

Mariarosaria Taddeo and Luciano Floridi

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 inforsphere and of the entities inhabiting it (LoA_{For}).

M. Taddeo (✉) • L. Floridi
Oxford Internet Institute, University of Oxford, Oxford, UK

Alan Turing Institute, London, UK
e-mail: mariarosaria.taddeo@oii.ox.ac.uk; luciano.floridi@oii.ox.ac.uk

M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*,
Law, Governance and Technology Series 31, DOI 10.1007/978-3-319-47852-4_2

2.1 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 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 ($\mathrm{LoA}_{\mathrm{IN}}$), while the other will focus on moral responsibilities *on* the web ($\mathrm{LoA}_{\mathrm{ON}}$). The former pertains to the regulation of the content available online. $\mathrm{LoA}_{\mathrm{IN}}$ highlights issues concerning information filtering, freedom of speech, censorship, and privacy. At $\mathrm{LoA}_{\mathrm{ON}}$, 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. 2.1). OSPs are often seen as *information gatekeepers* (Calhoun 2002) (more on this in Sect. 2.1), 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

> 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 $\mathrm{LoA}_{\mathrm{IN}}$.

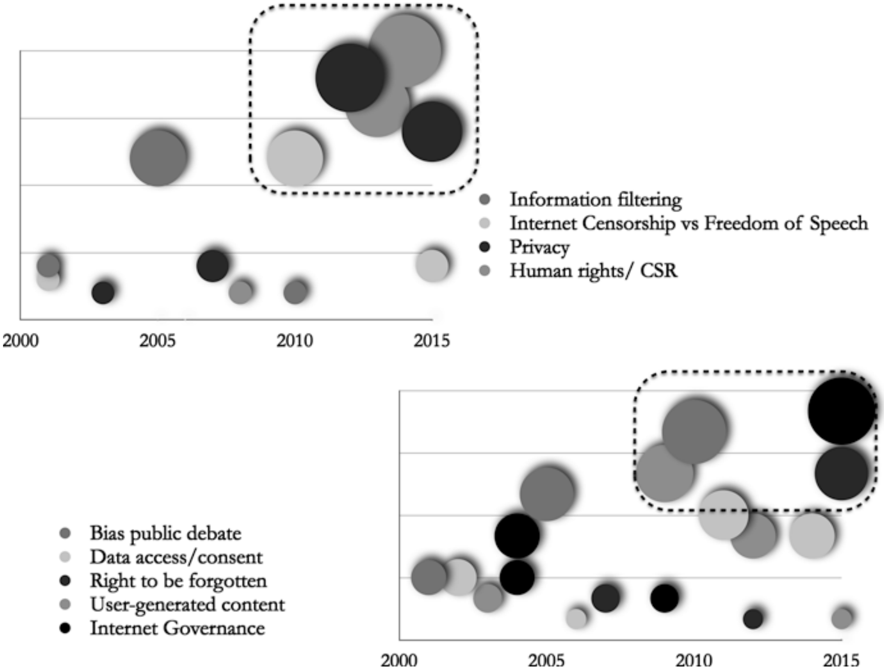

Fig. 2.1 The two graphs show some of the most relevant topics concerning the responsibilities of OSPs addressed in the literature in the past 15 years. The size of the circles is proportional to the number of research articles, books, and edited volumes that include either in the title or in the keywords 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.[4]

2.2 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.[5] 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

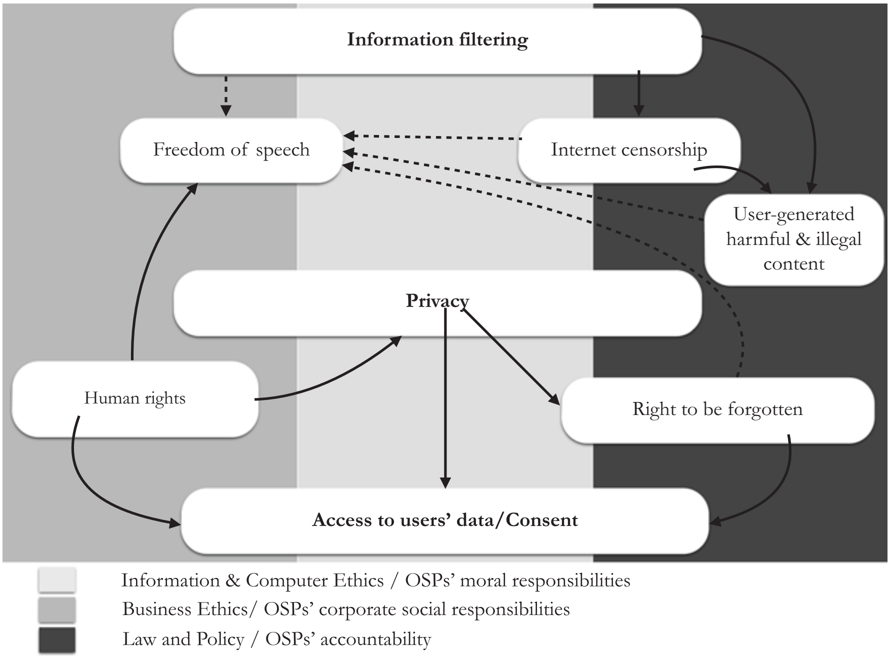
Information filtering
Freedom of speech
Internet censorship
User-generated harmful & illegal content
Privacy
Human rights
Right to be forgotten
Access to users' data/Consent
Information & Computer Ethics / OSPs' moral responsibilities
Business Ethics/ OSPs' corporate social responsibilities
Law and Policy / OSPs' accountability

Fig. 2.2 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.

overlapping areas (Fig. 2.2) more easily. Let us begin by focusing on online information filtering.

2.2.1 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 (Introna and Nissenbaum 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.[6] 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. 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)[7]. 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 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 2007; 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 (Sunstein 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),[8] 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 (Pariser 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. 2.1). 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, policymakers, 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).

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.[9] The regulation of user-generated content available online offers a good example of the case in point. The next section focuses on this topic.

2.2.2 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.[10] 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.[11] 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.[12]

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.[13] 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.[14] 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 (Vedder 2001) delves into this issue and suggests that OSPs should be held morally responsible for the dissemination of harmful content. The article 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 (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.[15] 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, Vinton Cerf (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.[16] 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.

2.2.2.1 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.[17] 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[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.[18]

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