UNESCO Publishing

United Nations
Educational, Scientific and
Cultural Organization

FOSTERING FREEDOM ONLINE

The Role of Internet Intermediaries

Rebecca MacKinnon • Elonnai Hickok • Allon Bar • Hae-in Lim

UNESCO SERIES ON INTERNET FREEDOM

FOSTERING FREEDOM ONLINE

The Role of Internet Intermediaries

Rebecca MacKinnon • Elonnai Hickok • Allon Bar • Hae-in Lim

A report prepared for UNESCO's Division for Freedom of Expression and Media Development. The opinions expressed in this report are those of the authors and do not necessarily reflect the views of UNESCO of its Division for Freedom of Expression and Media Development.

Published by the United Nations Educational, Scientific and Cultural Organization (UNESCO), 7 place de Fontenoy, 75352 Paris 07 SP, France, and the Internet Society, 1775 Wiehle Avenue, Suite 201, Reston, VA 20190-5108, United States.

UNESCO ISBN 978-92-3-100039-3

Typeset by UNESCO
Printed by UNESCO
Printed in France

FOSTERING FREEDOM ONLINE: THE ROLE OF INTERNET INTERMEDIARIES

Authors:

Rebecca MacKinnon, Director of the Ranking Digital Rights Project, New America Foundation; Visiting Affiliate, Center for Global Communication Studies at the Annenberg School for Communication, University of Pennsylvania

Elonnai Hickok, Centre for Internet and Society, Bangalore

Allon Bar, Ranking Digital Rights Project

Hae-in Lim, Ranking Digital Rights Project

Researchers:

Sara Alsherif, Researcher, Freedom of Information Program, Support for Information Technology Center, Cairo

Celina Beatriz Mendes de Almeida Bottino, Instituto de Tecnologia & Sociedade do Rio de Janeiro, Rio de Janeiro

Richard Danbury, Centre for Intellectual Property and Information Law, University of Cambridge

Elisabetta Ferrari, Center for Media, Data and Society, Central European University, Budapest; Annenberg School for Communication, University of Pennsylvania

Grace Githaiga, Kenya ICT Action Network (KICTANet)

Kirsten Gollatz, Alexander von Humboldt Institute for Internet and Society, Berlin

Elonnai Hickok, Center for Internet and Society, Bangalore

Hu Yong, Peking University

Tatiana Indina, Center for the Study of New Media and Society, Moscow

Victor Kapiyo, The Kenyan Section of the International Commission of Jurists (ICJ Kenya); Kenya ICT Action Network (KICTANet)

Peter Micek, Access, New York

Agustín Rossi, European University Institute, Florence; Global Public Policy Institute, Berlin

Table of Contents

Foreword

UNESCO, as enshrined in its Constitution, promotes the "free flow of ideas by word and image", and is accordingly committed to enabling a free, open and accessible Internet space as part of promoting comprehensive freedom of expression online and offline.

With the rise of Internet intermediaries that play a mediating role on the internet between authors of content and audiences, UNESCO is interested in how this recent historical phenomenon impacts on freedom of expression and associated fundamental rights such as privacy. This interest is linked to our draft conceptual framework of "Internet universality" which draws from UNESCO decisions on the Internet, and recognises that four core principles should inform cyber actors. These principles are that the Internet should be human **r**ights-based, **o**pen, **a**ccessible for all and governed by **m**ulti-stakeholder participation.

The full range of intermediaries includes search engines and internet-service providers (ISPs), hosting providers, cloud computing service through to online social networks, and media houses which provide for user-generated comment such as comments, blogs or citizen-journalism posts. These actors can enable freedom of expression in historically unprecedented ways, but all of them also face challenges when it comes to dealing with content which may transgress international standards for freedom of expression, be illegal in terms of national laws, be legal but merit certain restrictions because of ethical considerations, or be offensive in some eyes but not attracting restriction.

The decisions made by the diverse intermediaries on these pressing issues are partly shaped by the legal liability regime that applies to the different kinds of service or role provided. But there are also spaces where these actors make significant decisions within a given law, where they contest a number of legal measures, and where they seek the clarity of rule of law and one which is guided by international standards on free expression and privacy.

Though these issues have been hotly debated in past years, there is still a lack of empirical study highlighting the global complexity of the subject. This report fills the gap by collecting and analyzing empirical data around practices with regard to monitoring, surveillance, blocking, privacy-anonymity and take-down of content, and developing best practice recommendations from these.

UNESCO has been pleased to work on this research project with the Open Society Foundations, the Internet Society, and the Center for Global Communication Studies at the University of Pennsylvania's Annenberg School for Communication. The result is a scholarly document that is based on a case study methodology. It is a resource which enables the assessment of Internet intermediaries decisions on freedom of expression, by ensuring that any limitations are consistent with international standards.

UNESCO has succeeded in raising awareness and promoting good practice through past research in the UNESCO Series on Internet Freedom: *Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet (2011)* and *Global survey on Internet Privacy and Freedom of Expression (2012*).

We believe the rich material in this, the third in UNESCO's Series on Internet Freedom, will be of great value to all stakeholders. These are industry actors, UNESCO Member States, technical community, Intergovernmental organizations, private sector, civil society, and others both national and international.

The research also helps to inform UNESCO's implementation of a comprehensive and consultative multi-stakeholder Internet study as mandated by the Organization's 37th General Conference Resolution 52. The study, due in 2015, covers UNESCO's key competence areas of access to information and knowledge, freedom of expression, privacy, and ethical dimensions of the information society, and contains possible options for future actions.

Rich as it is, this report only covers three intermediary types - Internet Service Providers, Search Engines and Social Media. It will be followed by future studies on other intermediary types, including data processing, web hosting providers, cloud computing services, and domain name registries, as well as online media with substantial user-generated content.

UNESCO expresses its thanks to 16 international researchers led by Ms Rebecca MacKinnon and Mr Allon Bar, as well as 14 members of an International Advisory Committee, who have jointly delivered this work. UNESCO also thanks Mr Edward Pittman from the Open Society Foundations, Mr Nicolas Seidler from the Internet Society and Mr Monroe Price from the Center for Global Communication Studies at the University of Pennsylvania's Annenberg School for Communication, for their institutions' financial contributions and administrative support to the research.

Getachew Engida
Deputy Director-General of UNESCO

Executive summary

Freedom of expression is a universal human right that applies equally to the internet as to the offline world.[1]

As an international intergovernmental organization with a global remit that promotes universal values, UNESCO is exploring a conceptual framework of internet 'universality' according to which respect for four core principles is a precondition for the Internet to be universal: human **r**ights, **o**penness, **a**ccessibility; and **m**ultistakeholder participation. The four can be summarized by the mnemonic R – O – A – M (Rights-based, Open, Accessible, Multistakeholder driven).[2] This report addresses challenges for realizing the first principle, human rights. The research also helps to inform UNESCO's implementation of a comprehensive and consultative multi-stakeholder Internet study as mandated by the Organization's 37th General Conference Resolution 52.[3]

The goal of this report is to shed light on how internet intermediaries – services that mediate online communication and enable various forms of online expression – both foster and restrict freedom of expression across a range of jurisdictions, circumstances, technologies, and business models.

All of the intermediaries studied in this report are operated by companies. According to the UN Guiding Principles for Business and Human Rights, states have the primary duty to protect human rights, businesses have a responsibility to respect human rights, and both must play a role in providing remedy to those whose rights have been violated.[4]

The report's authors have applied this 'protect, respect, and remedy' framework to the policies and practices of companies representing three intermediary types (internet service providers, search engines, and social networking platforms) across ten countries. The three case studies highlight challenges and opportunities for different types of intermediaries in respecting and protecting online freedom of expression.

---

1 United Nations Human Rights Council. 16 July 2012. The promotion, protection and enjoyment of human rights on the Internet. United Nations Human Rights Council (A/HRC/RES/20/8). http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8

2 UNESCO. July 2014. Internet Universality: A Means towards Building Knowledge Societies and the Post-2015 Sustainable Development Agenda. Draft Proposed by the Secretariat. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/internet_universality_summary_240314_en.pdf

3 UNESCO General Conference. November 2013. 37 C/Resolution 52. Internet related issues: including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/37gc_resolution_internet.pdf

4 *Guiding Principles on Business and Human Rights*. 2011. Geneva, United Nations, p. 4. www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Findings

Operations of internet intermediaries are heavily influenced by the legal and policy environments of states. Research findings highlight the extent to which state policies, laws, and regulations – to varying degrees – are inadequately aligned with their duty to facilitate and support intermediaries' respect for freedom of expression. At the same time, the three case studies also document the extent to which companies are able to control many aspects of their policies and practices affecting online expression.

There is currently a trend among some internet intermediaries called 'transparency reporting': the disclosure of information about government and other lawful requests to restrict content, hand over user data or comply with other surveillance-related requirements. This report uses the term "requests" to cover the broad range of instructions, injunctions and demands made on intermediaries. There is also a movement among human rights advocates from a range of countries, some companies, and some investors calling for greater transparency by governments about requests being made of companies. Regarding these transparency-related trends this report contains two over-arching findings:

1. To the extent that intermediaries and governments have grown more transparent about requests made by governments to companies, there is much more transparency about surveillance and user data requests (directly affecting internet users' privacy) than about demands to restrict content and block communications.

2. For those intermediaries that publish 'transparency reports', disclosure has been largely limited to government or other demands made through legal processes, and the companies' handling of such demands. Few efforts have been made thus far by intermediaries to be more transparent about extra-legal content restrictions, as well as content removal and account deactivation and other actions taken to enforce intermediaries' own self-regulatory terms of service. Corporate transparency around collective self-regulatory efforts was also found to lag behind transparency related to direct government requests.

More specific findings of the three case studies can be summarized as follows:

***STUDY 1: Internet Service Providers (*fixed line and mobile) - Vodafone (UK, Germany, Egypt), Vivo/Telefônica Brasil (Brazil), Bharti Airtel (India, Kenya), Safaricom (Kenya)**
Across jurisdictions, stakeholders interviewed for this report highlighted the importance of ISPs and their key role in enabling expression. At the same time, ISPs can be a single point of failure for expression online particularly when content or entire services are filtered (blocked from being accessed by the user) or networks are shut down locally or nationally. Because ISPs must be physically present in a country in order to provide service and operate, the extent to which they facilitate or restrict freedom of expression is most directly affected by laws, regulations, and government actions compared to the other intermediaries studied. Findings include:

- Levels of transparency on matters related to privacy and surveillance are very low. Respect and protection of privacy by companies and governments is an enabler of freedom of expression.[5] Yet some companies studied do not have publicly available privacy policies for their core services in some countries. Data protection practices varied widely in tandem with whether or not countries had data protection laws. Few companies make an effort to be transparent about how they respond to government requests, or speak up for their users, even in relatively open political and media environments.
- Governments and companies offer even less transparency about restrictions of content and user expression made by and through ISPs than about policies and practices related to privacy and surveillance. This includes filtering and network shutdowns. "Self-regulatory" filtering processes suffer from questions about public accountability in their decision making about what content to restrict.
- With the emergence of an initiative called the Telecommunications Industry Dialogue, the two member companies included in this report Vodafone and (to a much more general degree) Telefonica have made public commitments to respect user rights, advocate for users with governments, and be more transparent. Because these commitments have just begun to be implemented, it is too early to know the concrete impact of these commitments on users' freedom of expression.

STUDY 2: Search Engines **- Google (USA, EU, India, China, Russia), Baidu (China), Yandex (Russia)** Search engines are a principal means by which internet users find and access information. Thus, their policies and practices affecting what content can or cannot be found online have major implications for freedom of expression. Of the companies studied, researchers found that search engines' policies and practices related to content restriction and manipulation are shaped by their home jurisdictions and to varying degrees by other jurisdictions in which they operate. Findings include:

- Differences in ISP filtering regimes have a strong influence on how, and to what extent, search engines restrict their own search results. For example, due to substantial difference in the technical and legal characteristics of filtering in Russia and China, Yandex and Baidu have very different restriction practices, and Google has taken different approaches to the two markets (remaining in Russia as of August 2014 but removing its operations from China since 2010).
- The stricter the intermediary liability regime in a given jurisdiction, the more likely content is to be removed either proactively by the company or upon request by authorities without challenge. Without government transparency, company transparency reports (Google was the only one of the three search engines studied) are the only way for users to ascertain the extent and nature of requests being made.
- While search engines carry out content restriction on government request, they also restrict or modify search results for many other commercial and self-regulatory

5 Navi Pillay. 30 June 2014. The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights. (A/HRC/27/37), p. 15. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

reasons, including user personalization and enforcement of companies' own rules about what content is acceptable to appear on their services.

STUDY 3: Social Networking Platforms **- Facebook (USA, Germany, India, Brazil, Egypt), Twitter (USA, Kenya), Weibo (China), iWiW (Hungary)** Social networking platforms have significantly lowered the threshold for individuals to publish content that can reach large audiences. For the two platforms with international user bases (Facebook and Twitter), researchers identified tensions between the companies' own policies and practices and governments' laws and regulations. The policies and practices of the more domestically focused platforms more closely mirror home governments' expectations and requirements. Findings include:

- Transparency reports published by Facebook and Twitter reveal the extent to which intermediary liability regimes affect the volume of government requests that companies receive to hand over user data and restrict content. The reports also reveal that companies have legal cause to decline a large percentage of requests made by many governments.
- The two companies studied that publish transparency reports define and categorize data in different ways, and choose to reveal or not reveal different types of information, making reports difficult to compare. Also, companies are much more transparent about how they respond to government requests than they are about the nature and volume of content restricted for violation of their own private rules.
- There is significant concern amongst some human rights advocates, including for example those working to stop gender-based violence and online hate speech, about companies' lack of communication with users about how terms of service are developed, interpreted and enforced.
- Given the significant amount of personal information collected by social networking platforms, these intermediaries have a special responsibility to take steps to anticipate harms to user privacy and to take steps to mitigate them.
- Even in countries with strict intermediary liability laws where companies face strong pressure from authorities to proactively restrict content and hand over user data, there are measures companies can take to be more transparent and demonstrate respect for users' rights. These include taking maximum possible steps to inform users when content is restricted, and also under what circumstances their personal information is collected and how it is shared.

Recommendations:

The report recommends specific ways that intermediaries can improve respect for internet users' right to freedom of expression. It also offers recommendations for states to support and facilitate intermediaries' respect for users' rights. Key recommendations include:

- **Adequate legal frameworks and policies:** Laws and regulations governing intermediaries should be consistent with international human rights norms, including the right to freedom of expression;
- **Multistakeholder policy development:** Laws, regulations and **governmental** policies, as well as **corporate** policies and rules, should be developed in consultation with all affected stakeholders;
- **Transparency:** Legitimacy and public trust depends on demonstrating that governance and enforcement actions – whether in accordance with the law or enforcement of intermediaries' own terms of service – are in compliance with pre-specified principles, rules and conditions. Transparency reporting and other actions to communicate with the public about company policy and practice should be comprehensive and sufficiently standardized so that it is possible to compare and analyze datasets across multiple companies.
- **Privacy:** Protecting internet users' right to privacy via intermediaries is essential for the flourishing of freedom of expression. Data protection regimes at the national level are vital, as are legal frameworks and other mechanisms to ensure that government access to user data and company practices in handling government requests are based on strict principles of necessity, proportionality, and accountability in terms of remedial mechanisms.
- **Accountability in self-regulation:** Intermediaries' private rules and accompanying enforcement processes, as well as government-supported efforts by companies to collectively self-regulate, should be compatible with human rights norms, including the right to freedom of expression. They should adhere to core principles of accountability, transparency and due process.
- **Remedy:** It should be possible for people to report grievances and obtain redress from private intermediaries as well as from state authorities, including from national-level human rights institutions.
- **Public information and education:** In order for freedom of expression to be protected and respected online, governments and companies have a responsibility to consult with stakeholders on their laws and rules and explain them clearly. They also have an obligation to educate users about their rights so that people can understand and effectively exercise them; recognize when their rights have been restricted, violated, or otherwise interfered with; and know where and how to report grievances and seek redress.
- **Global accountability mechanisms:** New structures such as the multistakeholder Global Network Initiative and the industry-organized Telecommunications Industry Dialogue have begun to have an impact on concrete commitments by companies to respect user rights and implement relevant policies and practices. Stakeholders concerned with protecting online freedom of expression should consider how to support and broaden global mechanisms that strengthen the incentives and capacity for intermediaries to respect internet users' rights, particularly in the area of self-regulation.

1. INTRODUCTION

Consider three recent developments and their implications for online freedom of expression around the world:

On 3 April 2014, the Turkish Government lifted a two-week block on the social networking service Twitter, after the Constitutional Court of Turkey, the country's highest legal body, ruled that the ban violated the right to freedom of expression. Although it successfully contested the block in court, Twitter did agree to restrict an account accusing a former minister of corruption by making the account inaccessible to internet users with IP addresses originating from Turkey. The account and its contents remained visible to everyone else in the world.[6]

On 13 May 2014, the Court of Justice of the European Union (CJEU) ruled that Google must respect the 'right to be forgotten' and enable individuals to request the removal from its search engine of links that were 'inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed'.[7] While the long-term impact of the CJEU decision has yet to play out, critics expressed concern that politicians and other powerful public figures would abuse this right to the detriment of freedom of expression.[8]

On 6 June 2014, in the period subsequent to Edward Snowden, a former contractor for the United States National Security Agency (NSA) releasing his first revelations about the US Government's surveillance of domestic and global networks, Vodafone, the world's second-largest telecommunications company with 434 million customers worldwide,[9] released a report analysing 'law enforcement demands received based on data gathered from [Vodafone's] local licensed communications operators' in the 29 countries in which it operates.'[10] Most relevant from the point of view of international standards for the right

6 Ceylan Yeginsu. 4 April 2014. Turkey Lifts Twitter Ban After Court Calls It Illegal. New York Times. www.nytimes.com/2014/04/04/world/middleeast/turkey-lifts-ban-on-twitter.html (Accessed 16 July 2014.)

7 Alan Travis and Charles Arthur. 13 May 2014. EU court backs 'right to be forgotten': Google must amend results on request. The Guardian. www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results (Accessed 16 July 2014.)

8 Mark Stephens. 18 May 2014. Only the powerful will benefit from the 'right to be forgotten'. The Guardian. www.theguardian.com/commentisfree/2014/may/18/powerful-benefit-right-to-be-forgotten (accessed 16 July 2014.)

9 Vodafone Group Plc. 20 May 2014. Empowering everybody to be confidently connected: Annual Report 2014. England, Vodafone, p. 1. www.vodafone.com/content/annualreport/annual_report14/downloads/full_annual_report_2014.pdf

10 Vodafone Group Plc. 20 May 2014. Law Enforcement Disclosure Report. www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

to privacy,Vodafone revealed that in six of those countries, government authorities can tap directly into the company's networks.[11]

Google's search engine, Twitter's social network, and Vodafone's telecommunication and internet services **are called internet intermediaries because they mediate online communication and enable various forms of online expression.** However, intermediaries can also act as chokepoints, arbiters or 'gatekeepers' of expression.[12] This powerful role prompted one legal scholar to write that 'Internet intermediaries govern online life'.[13] A recent book on the internet and human rights by one of this report's authors calls them 'sovereigns of cyberspace'.[14]

Yet intermediaries' power can only be fully understood in the context of state power. The position of internet intermediaries in relation to states and to international human rights standards is complicated: Internet intermediaries often operate across a variety of jurisdictions, and states expect them to comply with national laws that in turn align in varying degrees with international human rights norms. Optimists have regarded these companies as a source of 'liberation technology' that will help unshackle the hands of the oppressed.[15] Others have critiqued them for failing to protect user privacy rights and facilitating unaccountable surveillance by the private sector as well as governments.[16]

Intermediaries clearly have a powerful and positive role to play in fostering rights. However as this report will show, in order to protect freedom of expression, they need to follow international standards of transparency, necessity, proportionality, legitimate purpose, and due process in order not to engage in violation of rights.

1.1 Freedom of Expression Online

Freedom of expression is established under Article 19 of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).[17] Article 19 of the UDHR reads:

---

11 Amy Thomson and Danielle Lepido. 6 June 2014. Vodafone Prompts Protests Over Government Wiretapping. Bloomberg. www.bloomberg.com/news/2014-06-06/vodafone-says-29-governments-ask-for-access-to-its-user-data.html (Accessed 16 July 2014); Vodafone Law Enforcement Disclosure Report. op. cit.

12 Jonathan Zittrain. Spring 2006. A History of Online Gatekeeping. Harvard Journal of Law & Technology, Vol. 19, No. 2, pp. 253–98. http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf

13 Frank A. Pasquale. 2010. Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries. Northwestern University Law Review, Vol. 104, No. 1, p. 105. www.law.northwestern.edu/lawreview/v104/n1/105/LR104n1Pasquale.pdf

14 Rebecca MacKinnon. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, New York, Basic Books, pp. 6, 115–68.

15 Larry Diamond. July 2010. Liberation technology. *Journal of Democracy*, Vol. 21, No. 3, pp. 69–83. www.journalofdemocracy.org/articles/gratis/Diamond-21-3.pdf

16 Bruce Schneier. 20 November 2013. 'Stalker economy' here to stay. *CNN*. http://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html (Accessed 17 July 2014.)

17 Office of the United Nations High Commissioner for Human Rights. 23 March 1976. International Covenant on Civil and Political Rights. www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[18]

This right therefore covers the freedom to express and publish content as well as to have access to such content. As such, it provides for the right to press freedom and the right to information, and these apply across media platforms and national frontiers. International standards require that any limitations of these rights should be exceptions to the norm, and be based on legitimate purposes as set out in the UDHR and ICCPR. Likewise, limitations of any right need further to made be in terms of law, and be necessary and proportionate.

In 2012 the United Nations Human Rights Council adopted a landmark resolution affirming that 'the same rights that people have offline must also be protected online'.[19] It acknowledged the 2011 reports on 'the right to freedom of opinion and expression exercised through the Internet' by UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression Frank La Rue, which highlighted how freedom of expression can be fostered as well as violated through the internet.[20] La Rue warned of 'increased restrictions on the Internet through the use of increasingly sophisticated technologies to block content, monitor and identify activists and critics, criminalization of legitimate expression, and adoption of restrictive legislation to justify such measures'.[21]

In early June 2013, in the period before Snowden began to unveil revelations about the U.S. Government's surveillance, La Rue published another privacy-related document examining the impact of State surveillance on freedom of expression.[22] Especially relevant to this current report is La Rue's discussion of the private sector's key role in facilitating state surveillance, by 1) 'hav[ing] had to respond to requirements that digital networks and communications infrastructure be designed to enable intrusion by the State'; (2) 'developing and deploying new technologies and communications tools in specific ways'; or even (3) '[being] complicit in developing technologies that enable mass or invasive surveillance in contravention of existing legal standards'.[23]

---

18 United Nations. The Universal Declaration of Human Rights. www.un.org/en/documents/udhr Emphasis added.

19 United Nations Human Rights Council. 16 July 2012. The promotion, protection and enjoyment of human rights on the Internet. United Nations Human Rights Council (A/HRC/RES/20/8). http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8

20 Frank La Rue. 10 August 2011. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (United Nations General Assembly document A/66/290). www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf (Accessed 17 July 2014); Frank La Rue. 16 May 2011. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Office of the United Nations High Commissioner for Human Rights. (A/HRC/17/27). http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

21 A/HRC/17/27. p. 7.

22 Frank La Rue. 17 April 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Office of the United Nations High Commissioner for Human Rights. (A/HRC/23/40). www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

23 La Rue, A/HRC/23/40, op. cit., pp. 19–20.

La Rue also emphasized the importance of 'private, secure, and anonymous' communications, describing the 'chilling effect' of excluding individuals from vital social spheres and 'dissuading the free expression of information and ideas' when restrictions are placed on people's ability to communicate anonymously.[24] Later in 2013, La Rue's 'surveillance' report was further reinforced by a UN General Assembly resolution on the right to privacy in the digital age. It called on states to respect the right to privacy in digital communications and take measures to prevent violations, including a review of existing laws and practices and the establishment of oversight mechanisms.[25]

UNESCO follows the UN's position on human rights, based on the UDHR, and therefore the position that human rights are indivisible[26], recognizing thereby that particular actions concerning the right to privacy can impact on other rights, such as the right to freedom of expression, and vice versa. As stated in UNESCO's 37 C/Resolution 52, "privacy is essential to protect journalistic sources, which enable a society to benefit from investigative journalism, to strengthen good governance and the rule of law, and that such privacy should not be subject to arbitrary or unlawful interference".[27] At the same time, privacy may also not be used to shield violations of individual rights or to block the media from exposing these. Public interest must enter any calculation of reconciling rights.

This report builds on three UNESCO-commissioned works that have underscored the internet as an essential component of people's ability to exercise their right to freedom of expression, and written over the same time period as the developments described above. A 2011 UNESCO report called *Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet* provides an overview of the legal and regulatory contexts in which countries seek to balance the responsibility to protect freedom of expression with other rights, alongside other goals of the State, such as economic development, trade and industrial policy.[28] UNESCO's 2012 *Global Survey on Internet Privacy and Freedom of Expression* points out that poor privacy protection has a negative impact on freedom of expression.[29] UNESCO's 2014 report *World Trends in Freedom of Expression and Media Development* states that in addition to breaches of privacy, fear of reprisal also leads to self-censorship – by users as well as internet intermediaries.[30]

---

24 La Rue, A/HRC/23/40, op. cit., p. 7.

25 United Nations General Assembly. 20 November 2013. The right to privacy in the digital age. (UN Doc A/C.3/68/L.45/Rev.1. http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1

26 http://www.ohchr.org/en/issues/pages/whatarehumanrights.aspx

27 37 C/Resolution 52, ***Op. Cit.***

28 William H. Dutton, Anna Dopatka, Michael Hills, Ginette Law and Victoria Nash. 2011. ***Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet***. Paris, UNESCO Publishing. http://unesdoc.unesco.org/images/0019/001915/191594e.pdf

29 Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin and Natalia Torres. 2012. ***Global Survey on Internet Privacy and Freedom of Expression***. Paris, UNESCO Publishing, pp. 95–97. http://unesdoc.unesco.org/images/0021/002182/218273e.pdf

30 UNESCO. 2014. ***World Trends in Freedom of Expression and Media Development.*** Paris, UNESCO Publishing. http://unesdoc.unesco.org/images/0022/002270/227025e.pdf

Resolution 52 of the 37th General Conference in 2013 mandates UNESCO to conduct a comprehensive and consultative multi-stakeholder study on Internet-related issues within the mandate of UNESCO, including access to information and knowledge, freedom of expression, privacy, and ethical dimensions of the information society, and containing possible options for future actions. The results of this Study should inform the Organization's reporting on the implementation of the World Summit on the Information Society (WSIS) outcomes to the 38th General Conference in 2015. This research is conducted as an integral component of this ongoing exploration of Internet related issues within UNESCO's mandates.

1.2 Business and Human Rights

International human rights law has traditionally focused on state conduct. Its foundations are declarations drafted by and voted for by governments, and agreements concluded between states.[31] Over the past several decades, however, there is growing recognition that businesses also have human rights responsibilities for which they should be held accountable.

Because most internet intermediaries are operated by private-sector companies, this report builds on established human rights standards for business and human rights laid out by the UN's 'protect, respect and remedy' framework. It argues that governments have the primary duty to protect human rights, but companies also have a responsibility to respect human rights; both entities must ensure access to effective remedy.[32]

Building on that framework, in 2011 the Human Rights Council endorsed the Guiding Principles on Business and Human Rights, the result of six years of research and consultation with companies, governments and civil society by Prof. John Ruggie, the UN Special Representative of the Secretary-General on Business and Human Rights.

The Guiding Principles begin with the duty of States to protect against human rights abuses by businesses operating within their territory, and to 'set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operation.'[33]

The Guiding Principles outline three concrete steps for companies:[34]

1. Make a 'policy commitment to meet their responsibility to respect human rights';

---

31 Philip Alston. 2005.The 'Not-a-cat' Syndrome: Can the International Human Rights Regime Accommodate Non-State Actors? Philip Alston (ed.), *Non-State Actors and Human Rights*. Oxford, Oxford University Press, pp. 3-4.

32 Business and Human Rights Resource Centre. September 2010. The UN 'Protect, Respect and Remedy' Framework for Business and Human Rights. www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-protect-respect-remedy-framework.pdf

33 *Guiding Principles on Business and Human Rights*. 2011. Geneva, United Nations, p. 4. www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

34 Ibid, pp. 13–28.

2. Develop a 'human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights';

3. Initiate 'processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute'.

These principles apply to all companies – not just internet intermediaries. They also apply universally. As UN High Commissioner for Human Rights Navi Pillay wrote in her June 2014 report to the General Assembly, 'The responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations'.[35]

This report seeks to explain what internet intermediaries can do to maximize freedom of expression across a range of jurisdictions, circumstances, technologies and business models.

1.3 Intermediaries

An intermediary is 'any entity that enables the communication of information from one party to another.'[36] In a 2010 report, the Organisation for Economic Co-operation and Development (OECD) explains that internet intermediaries '**bring together or facilitate transactions between third parties on the Internet.** They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.'[37]

It is important to note that **most definitions of intermediaries explicitly exclude content producers**, as does this report. More explicitly, the OECD excludes from the intermediary's function 'activities where service providers give access to, host, transmit or index content or services that they themselves originate.'[38] In other words, in this view, publishers and other media that create and disseminate original content are *not* intermediaries. Examples of such entities include news websites that publish articles written and edited by staff or invited contributors, or a digital-video subscription service that hires or invites people to produce videos and then disseminates them to subscribers.

---

35 A/HRC/27/37. p. 15; Cynthia M. Wong. 25 July 2014. A Clear-Eyed Look at Mass Surveillance. Human Rights Watch. www.hrw.org/news/2014/07/25/clear-eyed-look-mass-surveillance (Accessed 3 August 2014); Nancy Scola. 16 July 2014. U.N. human rights chief: Surveillance is now world's 'dangerous habit'. *Washington Post*. www.washingtonpost.com/blogs/the-switch/wp/2014/07/16/u-n-human-rights-chief-surveillance-is-now-worlds-dangerous-habit (Accessed 3 August 2014.)

36 Thomas F. Cotter. 2005. Some Observations on the Law and Economics of Intermediaries. *Michigan State Law Review*, Vol. 1, p. 2. (Washington & Lee Legal Studies Paper No. 2005-14). http://ssrn.com/abstract=822987

37 Karine Perset/OECD. March 2010. *The Economic and Social Role of Internet Intermediaries*. Paris, Organisation for Economic and Co-operation and Development, p. 9. (DSTI/ICCP(2009)9/FINAL.) www.oecd.org/internet/ieconomy/44949023.pdf The report also credits internet intermediaries with 'provid[ing] the Internet's basic infrastructure and platforms by enabling communications and transactions between third parties as well as applications and services'. p. 6.

38 Perset/OECD, op. cit., p. 10.

At the same time, many entities offer hybrid services and constitute intermediaries to one extent or another. (This is particularly the case with traditional media organizations that also provide social networking or facilitate the sharing of user generated content, a type of hybrid intermediary not covered in this report.) To what extent social media services, for instance, are primarily intermediaries or also operate a media function, is important in terms of expectations. The Council of Europe has adopted a broad definition of media using six criteria to assess when new actors count as media. These criteria include intent to act as media, exercise of editorial control (with an editorial policy, process and staff), and application of professional standards. The effect of this is to recognise that, 'given media's needs and role in society, certain general provisions may need to be interpreted specifically for the media (for example in respect of defamation, surveillance, stop and search, state secrets or corporate confidentiality)…'. The Council of Europe's position also states that 'a differentiated and graduated approach requires that each actor whose services are identified as media or as an intermediary or auxiliary activity benefit from both the appropriate form (differentiated) and the appropriate level (graduated) of protection and that responsibility…'.[39]

Some stakeholders, however, have raised concerns that efforts by some states to define intermediaries as 'media' has resulted in stronger restriction on freedom of expression in a number of countries. Speaking at the 2014 Internet Governance Forum, one Google executive argued that in his company's experience 'the application of traditional media laws to this space' is 'used primarily as a way of stifling speech'.[40]

At the same time, all commercially operated Internet intermediaries studied in this report do require users to agree to 'terms of service' before they are allowed to use the service. Sometimes such terms may restrict users' speech that is actually protected by the law in some jurisdictions. (For example: Facebook and Twitter ban adult nudity and various forms of hate speech on their platforms in the United States even though most such content is not illegal in the US.) While the enforcement of such terms may resemble an editorial function, the legal basis for terms of service enforcement in the US and Europe (where internet intermediaries first emerged) is derived not from media law but from contract and commercial law, whereby companies have a right to require that users abide by terms of service in exchange for the provision of an online service operated by a private or commercial entity.[41]

---

39 Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media. (Adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies), https://wcd.coe.int/ViewDoc.jsp?id=1835645

40 Ross LaJeunesse, Global Head of Free Expression and International Relations, speaking on the panel 'Intermediaries' role and good practice in protecting FOE' 5 September 2014, Internet Governance Forum, Istanbul. For transcript and video see: http://www.intgovforum.org/cms/wks2014/index.php/proposal/view_public/21

41 See Ed Bayley. 16 November 2009. The Clicks that Bind: Ways Users "Agree" to Online Terms of Service. Electronic Frontier Foundation. https://www.eff.org/wp/clicks-bind-ways-users-agree-online-terms-service; Rustad, Michael L. and D'Angelo, Diane. 2012. The Path of Internet Law: An Annotated Guide to Legal Landmarks. *Duke Law & Technology Review*. Vol. 2011, No. 012. Suffolk University Law School Research Paper No. 11-18. Available at SSRN: http://ssrn.com/abstract=1799578; and Andrej Savin and Jan Trzaskowski, eds. Research Handbook on EU Internet Law. Edward Elgar Publishing. (Cheltenham, UK: 2014) pp. 414-415.

1.3.1 Types of Intermediaries

This report thus focuses on services and platforms that **host, give access to, index, or facilitate the transmission and sharing of content created by others**. As intermediaries' importance has grown not only for freedom of expression but also for the global knowledge economy, a number of organizations have sought to describe or categorize intermediary types by their roles and technical function. These include the OECD, the UN Special Rapporteur on Freedom of Expression, and civil society organizations such as Global Partners, Article 19 and the Center for Democracy and Technology. The table below provides a comparison of the key intermediary types that these organizations have characterized or singled out for examination.

Table 1: categories and key examples of Internet intermediaries

OECD[42]	Special Rapporteur La Rue[43]	Article 19[44]	CDT[45]	Global Partners[46]
Internet access and service providers	Internet service providers (ISPs)	Internet service providers (ISPs)	Access providers/ISPs Network operators and mobile telecommunications providers	Physical layer: makes communications possible
				Connectivity & code: the language or protocols of the communication
Data processing and web hosting providers		Web hosting providers	Domain registrars and registries Website hosting companies	Applications: tools to navigate content
Internet search engines and portals	Search engines	Search engines	Internet search engines and portals	
E-commerce intermediaries			E-commerce platforms and online marketplaces	
Internet payment systems				
Participative networking platforms	Blogging services Online communities Social media platforms	Social media platforms	Online service providers In general, any website that hosts user-generated content or allows user-to-user communications	

42 Perset/OECD, op. cit., p. 9.

43 "Intermediaries thus range from Internet service providers (ISPs) to search engines, and from blogging services to online community platforms." p. 11.

44 *Internet intermediaries: Dilemma of Liability*. 2013. London, Article 19, p. 3. www.article19.org/data/files/Intermediaries_ENGLISH.pdf

45 Kevin Bankston, David Sohn and Andrew McDiarmid. December 2012. *Shielding the Messengers: Protecting Platforms for Expression and Innovation*. Washington DC, Center for Democracy and Technology. www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf

46 Lisa Horner. 28 May 2008. A layer model for understanding the communications environment. *The Freedom of Expression Project*. www.freedomofexpression.org.uk/resources/shaping+a+public+interest+communications+environment (Accessed 17 July 2014.)

As reflected in by the table above, **different types of intermediaries perform different functions**. They also have different technical architectures. For example, **internet service providers** (ISPs) connect a user's device, whether it is a laptop, a mobile phone or something else, to the network of networks known as the internet. Once a user is connected to the internet, **web hosting providers** and **domain registrars and registries**, in turn, make it possible for websites to be published and to be accessed online. **Search engines** make a portion of the World Wide Web accessible by allowing individuals to search their database. Search engines are often an essential go-between between websites and internet users. **Social networks** connect individual internet users by allowing them to exchange text, photos, videos, as well as by allowing them to post content to their network of contacts, or to the public at large.

Different intermediary types further entail different kinds of business models. In order to provide internet access to people, telecommunications and ISPs must operate equipment and services within the geographical jurisdictions where those people physically reside. This type of service requires substantial investment of resources, equipment, and personnel in physical jurisdictions, requiring state permission and compliance with local law. Thus the relationship between ISPs and states is highly dependent, with states maintaining a high degree of leverage over them.

Telecommunications and internet access are not necessarily provided by the same actors. Internet service provision rides on the technical transmission infrastructure of telecommunication (wired or wireless or satellite) and which may serve as an underlying lever to exclude or limit access to certain ISPs or to their customers' users. In turn, the ISPs may limit access at a second level independently of their relationship with the telecommunications infrastructure operators. The reliance of ISPs on telecommunications makes the network level of intermediaries particularly susceptible to regulation by states.

By contrast, other intermediary types such as web hosting providers, domain name registrars and registries, search engines, and social networks do not necessarily need to locate staff, equipment or other physical resources in the same geographical area as the users they aim to serve. The open, interoperable architecture of the internet makes it possible for a user in Kenya or Egypt to conduct a search on Google, set up a website with a web hosting service, or communicate with friends on Facebook without those companies having staff, offices or equipment in those countries. This has the potential to remove web-based intermediaries – and their users – from control by states in which they are not headquartered or otherwise have a physical presence.

This independence is precisely why new media - particularly social media - have been documented by scholars as enhancing freedom of expression in contexts where offline expression is subject to strong restriction by the state.[47] In practice, however, a growing number of states are asserting jurisdiction over web-based intermediaries by exercising greater control over telecommunication and internet service providers as they serve as

47 Philip N. Howard. 2010. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*, Oxford, Oxford University Press; and Manuel Castells. 2012. *Networks of Outrage and Hope: Social Movements in the Internet Age*. Cambridge, Polity.

chokepoints for users to access the web.[48] States can – and increasingly do – threaten to deny access by all users under their jurisdiction to a particular service if web-based intermediaries fail to comply with their laws.[49]

Complementary to the issue of controlling intermediaries, states may also exercise control over users' online expression or access to information even outside the national jurisdiction. By targeting intermediaries, however, states are able to avoid the scale of directly policing individuals.

1.3.2 Modes of Restriction

Depending on the type of intermediary and the service offered, intermediaries control with whom and how their users can communicate. They have access to information created by users – such as posts, tweets, comments, blogs etc. – as well as a range of information directly related to users – such as registration details, private messages, search and browsing history, transaction details, location etc. For this reason, intermediaries are key in facilitating and protecting the rights to free expression and privacy. They also serve as avenues through which governments can monitor, regulate and control individuals' online activities and access to information. While the case studies will explain each mode of restriction in relationship to each intermediary type in greater depth, the three primary ways in which freedom of expression can be restricted via ISPs, search engines and social media can be broadly described as follows:

1. **At the network-level:** Telecommunications access providers and Internet service providers can restrict freedom of expression in three main ways:

    a. ***Filtering:*** Access is blocked to either entire websites, specific pages or specific keywords.[50] Filtering is carried out either by the ISP, or by the network operators that control internet flows into a jurisdiction, or some combination of the two. Such blocking prevents users from receiving information but can also prevent users from posting information to a specific location such as in the case of social networks. The content still exists elsewhere on the internet, but cannot be accessed by users of the network on which the filter is deployed.

    b. ***Service shutdown:*** One or more services offered by one provider or all providers can be shut down in a given jurisdiction or geographic area, preventing users in the area from accessing the internet via fixed line or mobile, sending SMS messages etc.

---

48 Chris Tuppen. 2012. *Opening the Lines: A Call for Transparency from Governments and Telecommunications Companies*. Global Network Initiative. https://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf

49 Rebecca MacKinnon. 3 February 2014. Playing Favorites. *Guernica*. www.guernicamag.com/features/playing-favorites (Accessed 17 July 2014.)

50 OpenNet Initiative. About Filtering. https://opennet.net/about-filtering (Accessed 17 July 2014.)

c. ***Non-neutral service:*** Access to certain content or applications is 'throttled' or slowed down, making it more difficult for users to access them. Alternatively, users might be charged different rates for access to different kinds of content or services, or might be granted free access to specific services.

The two other intermediary types covered by this report, search engines and social networks, are directly affected by these restrictions carried out at the network level. Importantly, **filtering or the threat of filtering at the network level is a means by which pressure can be placed on search engines, social networks and other intermediaries to carry out restrictions at the platform level.**

2. **At the platform level:** Intermediaries that operate at the platform level such as search engines and social networks can act to remove content completely, block it from view to particular categories of users (usually based on geography), or deactivate user accounts. These actions are carried out by the company itself or by government authorities who have been granted direct technical access to the platform's core functions.51 The removal, blocking, or deactivation may take place at the request of a government, at the request of users or other third parties, or according to the intermediary's own private rules and system of enforcement. (See Case Studies 2 and 3 for examples and details.)

The restrictions described above are an enforcement tool for different kinds of public and private governance: They are used to enforce state regulation or to help identify violations of state regulation. They can be used to enforce companies' private terms of service and other rules. They are also used in some countries to enforce standards issued by private or quasi-governmental bodies.

3. **Privacy-related (at both network and platform levels):** Internet users who believe that their communications and online behaviour is being monitored or exposed in a manner that violates their privacy rights are less likely to express themselves freely while using the services of internet intermediaries. Privacy can be negatively affected via all tiers of intermediaries in several ways:

   a. ***Data collection and monitoring*** through technologies such as deep packet inspection, takes place at all layers of the internet and has the ability to restrict expression through encouraging self-censorship.

   a. ***Lack of security in how user data is stored or how content data is transmitted*** can result in breaches of privacy, unauthorized interception, or interception by government authorities without the active involvement of the company.

---

51 Ethan Zuckerman. April 2010. Intermediary Censorship. Ronald Deibert (ed.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, Mass., MIT Press, pp. 71–85. www.access-controlled.net/wp-content/PDFs/chapter-5.pdf; Rebecca MacKinnon. 2 February 2009. China Censorship 2.0: How Companies Censor Bloggers. *First Monday*, Vol. 14, No. 2. http://firstmonday.org/article/view/2378/2089

a. ***User control over personal information:*** Different services and platforms provide internet users with varying levels of control over if and how their information is preserved or publicly accessible.

The following table provides a summary of the modes of restriction described above.

Table 2: Modes by which expression can be restricted via internet intermediaries either on request or on company initiative

	ISPs	Search Engines	Social Media
Network-level Restrictions	• Filtering • Service shutdown • Non-neutral service		
Platform-level restrictions		• Manipulation of search ranking • Removal or "de-listing" of links to specific web pages or categories of web pages	• Removal of content from the platform • Blocking of content, and free expression opportunities, by restricting access of particular categories of users (including geographical location) • Account limitation or deactivation
Privacy-related chilling effects	• Collection and retention of user data for commercial or government mandated purposes • "Real name" account registration requirements • State requests for user data • Real-time state surveillance	• Collection and retention of user data for commercial purposes • State requests for user data • Catalogue of individuals' personal individual via searches on their name	• Collection and retention of user data for commercial purposes • "Real-name" identity requirements • State requests for user data

The role that intermediaries play in protecting or restricting freedom of expression is further complicated by the global nature of many companies. Multinational companies, as well as internet services with users in multiple jurisdictions, can be subject to a global patchwork of legal and regulatory regimes. Some internet companies (including search engines and social networking platforms) have sought to address this dilemma by creating country specific filters – i.e. restricting access to content only in the jurisdiction where that content has been found illegal,[52] and by developing clear company policy on handling government requests for content restriction as well as user data requests.[53]

52 For example, Twitter filters content on a geographic basis. Dave Neal. 27 January 2012. Twitter to filter content geographically. *The Inquirer*. www.theinquirer.net/inquirer/news/2141809/twitter-filter-content-geographically (Accessed 17 July 2014.)

53 Global Network Initiative. Implementation Guidelines: Freedom of Expression. http://globalnetworkinitiative.org/implementationguidelines/index.php#29

When a company does not have any physical offices or personnel in a particular jurisdiction, it is difficult for a government to compel that company to abide by its laws or respond to its requests for content restriction. In response, some governments have resorted to filtering – or threatening to filter – content or entire services when a company -fails to comply with their requests to remove objectionable content.[54] In all this complexity, freedom of expression standards are often inadequately protected, respected and remedied.

1.3.3 Commitments to Freedom of Expression

In light of this increasingly complex global landscape, a number of efforts have emerged in recent years at the industry and governmental level to help internet intermediaries maximize respect for users' privacy and freedom of expression. For example, in 2013 the European Commission launched a 'sector guide' on how ICT companies in the ICT sector can implement the UN Guiding Principles, which were developed in consultation with industry, academia, civil society and governments.[55]

Some intermediaries have begun to make public commitments to respect users' rights. Since its launch in 2008, several internet companies have joined the Global Network Initiative (GNI), a multistakeholder body in which major intermediaries work together with participants from civil society, responsible investment, and academia to implement a set of core principles on freedom of expression and privacy.[56] Of the intermediaries studied in this report, Google is a founding member of the GNI and in January 2014 passed the organization's assessment process verifying that the company had satisfactorily implemented the GNI principles in handling government requests for content restriction and user data.57 Facebook joined the GNI in May 2013 but had not by August 2014 undergone an assessment to verify whether it has implemented the GNI principles.[58] In 2012, a group of telecommunications companies, including Vodafone, formed the Telecommunications Industry Dialogue on Freedom of Expression and Privacy in an effort

54 For example, in Brazil, a court threatened to block Facebook from the country for not removing content related to a dispute between two neighbours. Giancarlo Frosio. 7 October 2013. A Brazilian Judge Orders Facebook off Air If It Fails to Remove a Defamatory Discussion. Stanford Law School Center for Internet and Society blog. http://cyberlaw.stanford.edu/blog/2013/10/brazilian-judge-orders-facebook-air-if-it-fails-remove-defamatory-discussion (Accessed 17 July 2014.)

55 The Institute for Human Rights and Business and Shift. June 2013. ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights. European Commission, www.shiftproject.org/publication/european-commission-ict-sector-guide

56 Global Network Initiative. Principles: Freedom of Expression. http://www.globalnetworkinitiative.org/principles/index.php#18.

57 Global Network Initiative. January 2014. Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo. http://globalnetworkinitiative.org/sites/default/files/GNI%20Assessments%20Public%20Report.pdf

58 Evelyn M. Rusli. 22 May 2013. Facebook Joins GNI Online Privacy-and-Freedom Group. *Wall Street Journal* Digits blog. http://blogs.wsj.com/digits/2013/05/22/facebook-joins-gni-online-privacy-and-freedom-group (Accessed 17 July 2014); Alexandra Kulikova. 24 May 2013. Facebook Joins the Global Network Initiative – What to think of it? The London School of Economics and Political Science Media Policy Project blog. http://blogs.lse.ac.uk/mediapolicyproject/2013/05/24/facebook-joins-the-global-network-initiative-what-to-think-of-it (Accessed 17 July 2014.)

to develop principles and best practices most relevant to the business model of one category of intermediaries.[59]

A growing number of internet and telecommunications companies are also publishing regular 'transparency reports', thus named for the light they shed on the volume and nature of requests to remove content – whether by government or other private entities – or to disclose user data.[60] Such transparency helps users and the public at large understand what kinds of restrictions are being undertaken, and on whose behalf they are carried out. Among companies studied in this report, Facebook, Google, Twitter and Vodafone have published transparency reports. It is important to note, however, that significant variations in their scope, detail, and reporting methodology make it difficult to draw meaningful conclusions about one company's respect for free expression and privacy in comparison to another. Scholars have called on companies to work with academics and advocates to establish more standardized approaches to transparency reporting. They also propose that full transparency involves reporting more than just numbers of government requests received and complied with. Transparency about companies' policies and practices for handing government requests as well as private enforcement mechanisms are equally important.[61]

1.4 Methodology

This report presents three case studies examining three intermediary types. It covers 11 companies operating in ten countries:

CASE #1, Internet Service Providers and telecommunication services: Vodafone (UK, Germany, Egypt), Vivo/Telefônica Brasil (Brazil), Bharti Airtel (India, Kenya), Safaricom (Kenya)

CASE #2, Search Engines: Google (USA, EU, India, China, Russia), Baidu (China), Yandex (Russia)

CASE #3, Social Networks: Facebook (USA, Germany, India, Brazil, Egypt), Twitter (USA, Kenya) Weibo (China), iWiW (Hungary)

---

59 Peter Micek. 12 March 2013. Telecom Industry Dialogue to collaborate with GNI on freedom of expression, privacy rights. Access Now blog. https://www.accessnow.org/blog/2013/03/12/telco-industry-dialogue-to-collaborate-with-gni-on-freedom-of-expression-pr (Accessed 17 July 2014); Sarah A. Altschuller. 25 March 2013. Telecommunications Companies Release Guiding Principles on Freedom of Expression and Privacy. Foley Hoag LLP Corporate Social Responsibility and the Law blog. www.csrandthelaw.com/2013/03/25/telecommunications-companies-release-guiding-principles-on-freedom-of-expression-and-privacy (Accessed 17 July 2014.)

60 Danny Yadron. 15 May 2014. A Year After Snowden, Tech Companies Are More Transparent. Wall Street Journal Digits blog. http://blogs.wsj.com/digits/2014/05/15/a-year-after-snowden-tech-companies-are-more-transparent (Accessed 17 July 2014); Kashmir Hill. 14 November 2013. Thanks, Snowden! Now All The Major Tech Companies Reveal How Often They Give Data To Government. Forbes. www.forbes.com/sites/kashmirhill/2013/11/14/silicon-valley-data-handover-infographic (Accessed 17 July 2014.) Transparency Reports Database: Government Requests for User Data, https://transparency-reports.silk.co (Accessed 16 July 2014.)

61 Ryan Budish. 19 December 2013. What Transparency Reports Don't Tell Us. *The Atlantic*. www.theatlantic.com/technology/archive/2013/12/what-transparency-reports-dont-tell-us/282529 (Accessed 16 July 2014.)

The case studies are preceded by a description and analysis of the evolving legal and regulatory contexts in which internet intermediaries operate globally generally, and in the case study countries particularly. They are followed by general conclusions, plus recommendations for all stakeholders.

Africa and gender equality are the two top global priorities UNESCO's General Conference (its governing body) has identified for all its programmatic activities. Therefore Chapter 2 contains a special section on intermediary liability in Africa, Chapter 6 addresses gender issues involving internet intermediaries.[62]

Selection of the three different intermediary types was informed by the OECD's five-part classification of internet intermediaries, plus the three intermediary types singled out as examples in UN Special Rapporteur Frank La Rue's 2011 report on the right to freedom of opinion and expression on the Internet. (See 'Intermediaries: Definition and Types' in the Introduction above for a full discussion.)

Companies and countries of focus for each case were selected because they collectively represent a range of cultural, regional, political and legal environments from which powerful internet intermediaries have arisen – and within which these companies operate.

They cover a number of key markets:

- United States, the UK, and more generally the EU, where many of the world's largest internet and telecommunications companies are headquartered;
- Brazil, Russia, India and China – these so-called 'BRIC countries' that represent the leading emerging-market economies – and are an untapped, lucrative user base for global companies as well as the home base for successful national companies;
- Kenya, an African country with a relatively developed internet and telecommunications sector that has faced issues particularly related to hate speech;
- Egypt, where internet intermediaries are considered by participants and scholars to have been significant during the 2011 revolution;
- Hungary, a smaller market where an indigenous social network struggled to compete with global competitors.

For every country covered by the case studies, an in-country research team was commissioned to complete a detailed research questionnaire containing an average of 61 questions about the legal and political context affecting internet regulation, about the policies and practices of the selected companies in the selected countries, and also about how the combination of particular company policies and legal context affect internet users. Researchers were also asked to respond to several specific questions on gender.

62 UNESCO. 2013. *Draft Medium-Term Strategy: 2014–2021 (37 C/4)*. Paris, UNESCO Publishing, pp. 16–18. http://unesdoc.unesco.org/images/0022/002200/220031e.pdf

Researchers also conducted interviews with representatives from industry, government, civil society, academia and law. The questionnaires included questions about user perspectives in each country covered by the case studies. Researchers answered these questions by canvassing available academic research, media reports and relevant user forums.

The questionnaires were designed in consultation with the researchers in early 2014. Research for the questionnaires was then carried out in March and April 2014. The results of these questionnaires were then analysed and distilled by the report's authors. Based on this comparative analysis of the research questionnaires, an introductory chapter on regulation plus three case studies were drafted. The report's authors then worked with the researchers to clarify and update the research through July 2014.

It is important to note that resource and time constraints did not permit statistically meaningful user polling or in-depth user research through focus groups. Systematic, in-depth research on user perspectives at the national level on how different internet intermediaries shape people's online expression in different legal and regulatory contexts would be an important next step. Such a further research agenda could add to information for all stakeholders on how intermediaries can best be governed and operated in a manner that supports freedom of expression.

It is also important to keep in mind that this report only covers three intermediary types. The study of internet intermediaries will be further informed by future studies on other intermediary types, including data processing, web hosting providers, cloud computing services, and domain name registries, as well as online media with substantial user-generated content.

The next chapter will provide an overview of the legal and regulatory context shaping public and private regulation of the case study companies in the particular countries studied.

2. LAW AND REGULATION

Just as online platforms and services can be used for legitimate purposes including self-expression, education, employment, and trade, they can also be used for illegitimate purposes such as theft or fraud, harassment, copyright infringement, defamatory speech and so on. The line determining a legitimate and illegitimate purpose is significantly influenced by political, religious, and cultural context – resulting in multiple understandings of legitimate and illegitimate purposes throughout the world. Recognizing this tension, particularly in the context of speech, the UDHR, ICCPR and other international human rights instruments define limitations on the right to freedom of expression in order to protect other human rights. Yet as UN Special Rapporteur La Rue underscored in his 2011 report, restrictions are only compatible with international human rights standards when they meet three conditions:[63]

- The restriction must be rule-based, provided by law and carried out in a transparent and predictable manner;
- The restriction must be necessary and proportionate, using the least restrictive means to achieve the objective;
- The restriction must be consistent with purposes cited in the ICCPR: necessary to protect the rights or reputation of others, national security or public order, public health or public morals.

It is also important to note that the UN Human Rights Committee has determined that 'public morals' in the human rights context should be compatible with religious and ideological pluralism.[64] Restrictions applied by intermediaries should be evaluated in terms of these international standards. Evaluation should also be responsive to diverse legal regimes.

Intermediaries are sometimes held criminally liable for user content that others perceive as violating privacy or defamation laws [see 2.2 below]. In countries where that is the case, companies come under pressure to conduct their own monitoring and filtering to avoid possible repercussions. This contributes to a process of state-sanctioned self-regulation in which some governments may come to rely on private sector companies to regulate online content without public accountability or due process.[65] On the other hand, self-regulation may sometimes serve to protect freedom of expression and respect for the normative limitations on restriction as per the UDHR and ICCPR.

---

63 A/HRC/17/27. p. 8.

64 General Comment 34 on Office of the United Nations High Commissioner for Human Rights, Article 19, para. 32. www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc; *Irina Fedotova v. Russian Federation*, Office of the United Nations High Commissioner for Human Rights, para. 10. www2.ohchr.org/english/bodies/hrc/docs/CaseLaw/CCPR-C-106-D-1932-2010.doc

65 UNESCO. 2014. *World Trends in Freedom of Expression and Media Development*. op. cit. p. 33.

2.1 State Commitments and Limitations on Expression

The three case studies at the core of this report examine the operations of specific internet intermediaries in the context of specific legal jurisdictions: **Brazil**, **China**, **Egypt**, **Germany**, **Hungary**, **India**, **Kenya**, **Russia** the **United Kingdom** and the **United States**. This chapter gives a brief overview of the relevant legal and regulatory contexts of all jurisdictions and regions covered by the case studies.

While technology, business models and the scope of business carried out by internet intermediaries have evolved dramatically over the past two decades, the types of regulatory goals pursued by states remain largely unchanged, even if the methods used to pursue those goals have evolved along with the technology.[66] Below are some examples – though by no means a comprehensive list – of the types of regulatory objectives pursued by the states in the three case studies, which in turn have a direct impact on how (and to what extent) intermediaries are compelled to restrict freedom of expression online. In many instances, there is debate about the alignment of states' regulations to ICCPR standards and the implementations of these standards. While the types of limitations are often aligned with legitimate purpose, they often fall short in terms of the safeguards of necessity, proportionality and due legal process for implementation.

2.1.1 Types of Limitations

Defamation: Defamation laws seek to discourage unwarranted attacks on a person's reputation. UNESCO,[67] the UN Special Rapporteur,[68] the Organization for Security and Co-operation in Europe (OSCE)[69] and the Organization of American States have called for the decriminalization of defamation.[70] Nevertheless, **defamation remains criminalized in all of the countries examined in this report other than the United Kingdom and the United States**.[71]

---

66 Wolfgang Benedek and Matthias C. Kettemann. December 2013. *Freedom of Expression and the Internet*. Strasbourg, Council of Europe Publishing, pp. 45–54. https://book.coe.int/eur/en/human-rights-and-democracy/5810-freedom-of-expression-and-the-internet.html

67 UNESCO. 2014. *World Trends in Freedom of Expression and Media Development*. op. cit. pp. 27–30.

68 A/HRC/17/27. p. 11.

69 Organization for Security and Co-operation in Europe. Decriminalization of defamation. www.osce.org/fom/106287

70 United Nations Human Rights Committee. 26 April 2012. Communication No. 1815/2008 Views adopted by the Committee at its 103rd session, 17 October–4 November 2011. UN Doc CCPR/C/103/D/1815/2008/Rev.1, p. 9. www.worldcourts.com/hrc/eng/decisions/2011.10.26_Adonis_v_Philippines.pdf; Zsolt Bobis. 17 May 2012. Case Watch: When Telling the Truth May Come with A Prison Sentence. Open Society Justice Initiative Blog. www.opensocietyfoundations.org/voices/case-watch-when-telling-truth-may-come-prison-sentence (Accessed 3 August 2014.)

71 Article 19. Defamation maps (last updated 2012). www.article19.org/defamation/map.html (Accessed 30 July 2014); Yan Mei Ning. Summer 2011. Criminal Defamation in the New Media Environment – The Case of the People's Republic of China. *International Journal of Communications Law & Policy,* Vol. 14, pp. 6–14. http://ijclp.net/ojs/index.php/ijclp/article/view/15/5; Kayode Oladele. 27 August 2011. Internet Libel and the Law of Defamation: Justice Without Borders? *Sahara Reporters*. http://saharareporters.com/2011/08/27/internet-libel-and-law-defamation-justice-without-borders-kayode-oladele (Accessed 30 July 2014.)

National and public security: Different governments apply varying definitions, approaches and scope to 'national security' and 'public security'. In **China**, Article 15 of the 'Measures on the Administration of Internet Information Services',[72] promulgated by the State Council in 2000, stipulate what have come to be known as the 'nine forbidden content categories' for Chinese online services. These categories include speech that 'harms the dignity or interests of the State', or 'disseminates rumours, disturbs social order or disrupts social stability', or 'Sabotages State religious policy or propagates heretical teachings or feudal superstitions'.[73] **Egypt** restricts seditious speech as well as speech offensive of domestic and foreign governmental authorities.[74] The Egyptian Parliament has been considering an anti-terrorism law that would allow for internet companies and platforms to be blocked from the country for 'endangering public order'.[75] In **Russia**, the presidential amendment to the Law on Information (FL 398) allows the Prosecutor General's Office to blacklist any website it identifies as 'extremist propaganda' with the potential to incite anti-government riots, without a court order.[76] Russia also criminalizes the sharing of 'extremist' content on social networks.[77] **India** also allows for the restriction of online content by the central government or authorized authorities for national security reasons, including: in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of any cognizable offence relating to the above.[78] The **United States** prohibits incitement to 'imminent lawless action',[79] disclosing classified government information80 and 'knowingly provid[ing] material support or

---

72 People's Republic of China State Council. 25 September 2000. Measures on the Administration of Internet Information Service. People's Republic of China State Council Decree No. 292. www.net.cn/static/hosting/fa_xinxi.htm

73 People's Republic of China State Council. 25 September 2000. Measures. Op. cit.

74 Arab Republic of Egypt. August 1937. Penal Code No. 58 of 1937, Articles 98F, 102, 161, 179, 181, 185 and 186. http://www1.umn.edu/humanrts/research/Egypt/criminal-code.pdf

75 Alastair Sloan. 3 February 2014. Egypt's draft anti-terrorism law sparks concern about censorship. *Index on Censorship*. www.indexoncensorship.org/2014/02/egypts-draft-anti-terrorism-law-sparks-concern-censorship (Accessed 17 July 2014.)

76 Russian Duma Passes Bill On 'Website Blacklist' In Final Reading. 11 July 2012. *Radio Free Europe/Radio Liberty*. www.rferl.org/content/russia-passes-internet-bill/24642146.html (Accessed 17 July 2014); Russian Federation. 28 December 2013. Federal Law No. 398-FZ 'On Information, Information Technology and Information Protection. *Rossiiskaya Gazeta*. (In Russian.) www.rg.ru/2013/12/30/extrem-site-dok.html (Accessed 18 July 2014.)

77 Putin Signs Vaguely Worded Law Criminalizing Online 'Extremism'. 1 July 2014. *Radio Free Europe/Radio Liberty*. www.rferl.org/content/putin-extremism-internet-law-bill-rights/25441609.html (Accessed 18 July 2014); Putin Signs Law Giving Prison Terms for Internet Extremism. 30 June 2014. *The Moscow Times*. www.themoscowtimes.com/news/article/putin-signs-law-giving-prison-terms-for-internet-extremism/502717.html (Accessed 18 July 2014.)

78 Department of Electronics and Information Technology, Ministry of Communications and IT, Government of India. 5 Februay 2009. Indian Information Technology Act 2000 as amended in 2008 – Section 69A. http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

79 *Brandenburg v. Ohio*, 395 U.S. 444 (1969), www.oyez.org/cases/1960-1969/1968/1968_492 The Supreme Court also characterized some expression as not protectable under the First Amendment through doctrines as the 'fighting words' doctrine.

80 Legal Information Institute. 18 U.S. Code, Chapter 37 – Espionage and Censorship. Cornell University Law School. www.law.cornell.edu/uscode/text/18/part-I/chapter-37; Georgetown Law Library. National Security Law Research Guide. www.law.georgetown.edu/library/research/guides/national_security.cfm#v-statutes-and-legislative-history

resources to a foreign terrorist organization'.[81] The **United Kingdom** prohibits breaches of official secrets,[82] and expression that encourages terrorism or disseminates terrorist publications.[83] In 2010 the UK established the Counter Terrorism Internet Referral Unit (CTIRU), which reviews 'violent extremist or terrorist' content that the public submits through an anonymous online reporting tool and 'proactively scans the web for content that promotes or glorifies terrorism'.84 It then works with intermediaries to remove infringing content.[85]

Hate speech: The 2010 Constitution of **Kenya** prohibits incitement to violence, hate speech, advocacy of hatred that constitutes ethnic incitement, vilification of others, or incitement to cause harm, or is based on any ground of discrimination specified in the Constitution.[86] Article 13 of the National Cohesion and Integration Act 2008 prohibits 'threatening, abusive or insulting words or behaviour' with the intention of 'stir[ring] up ethnic hatred' (or that is likely to happen). Notably, the law only mentions ethnic hatred; there is no mention of religion, gender, nationality or sexual preference.[87] **Hungary** prohibits expression that violates another person's human dignity, the dignity of the Hungarian nation, or the dignity of any national, ethnic, or religious minority group.[88] The **United Kingdom** prohibits incitement to racial and religious hatred,[89] language that intentionally

---

81 *Holder v. Humanitarian Law Project, et al.,* 130 S. Ct. 2705 (2010), www.supremecourt.gov/opinions/09pdf/08-1498.pdf ; Adam Liptak. 22 June 2010. Court Affirms Ban on Aiding Groups Tied to Terror. *New York Times*. www.nytimes.com/2010/06/22/us/politics/22scotus.html?pagewanted=all (Accessed 30 July 2014); Adam Liptak. 11 February 2010. Right to Free Speech Collides With Fight Against Terror. *New York Times*. www.nytimes.com/2010/02/11/us/11law.html (Accessed 30 July 2014.)

82 UK Government. 1989. Official Secrets Act 1989. The National Archives. www.legislation.gov.uk/ukpga/1989/6/contents

83 UK Government. 2006. Terrorism Act 2006, Section 2: Dissemination of terrorist publications. The National Archives. www.legislation.gov.uk/ukpga/2006/11/section/2

84 Juliette Garside. 27 November 2013. Ministers will order ISPs to block terrorist and extremist websites. *The Guardian*. www.theguardian.com/uk-news/2013/nov/27/ministers-order-isps-block-terrorist-websites (Accessed 12 August 2014); Ines von Behr, Anaïs Reding, Charlie Edwards and Luke Gribbon. 2013. The use of the internet in 15 cases of terrorism and extremism. Cambridge, UK, RAND Corporation. pp. 4–6. www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf; Association of Chief Police Officers. The Counter Terrorism Internet Referral Unit. www.acpo.police.uk/ACPOBusinessAreas/PREVENT/TheCounterTerrorismInternetReferralUnit.aspx

85 Erin Marie Saltman. 23 May 2014. Jihad trending: Analysis of online extremism and how to counter it. *Index on Censorship*. www.indexoncensorship.org/2014/05/jihad-trending-comprehensive-analysis-online-extremism-counter (Accessed 12 August 2014.)

86 Republic of Kenya. Article 33(2), Constitution of Kenya, www.klrc.go.ke/index.php/constitution-of-kenya/112-chapter-four-the-bill-of-rights/part-2-rights-and-fundamental-freedoms/199-33-freedom-of-expression; Section 5B, Kenya Information and Communication Act, op. cit.

87 Umati Project. February and March 2013. Umati: Monitoring Online Dangerous Speech. iHub Research and Ushahidi. www.research.ihub.co.ke/uploads/2013/april/1365508815_819_823.pdf (Accessed 12 August 2014.)

88 Hungarian Government. 25 April 2011. Hungarian Fundamental Law, Article IX, paragraphs 4–5. www.kormany.hu/download/e/02/00000/The%20New%20Fundamental%20Law%20of%20Hungary.pdf

89 UK Government. 2006. Racial and Religious Hatred Act 2006 (RRHA). www.legislation.gov.uk/ukpga/2006/1; Q&A: Religious hatred law. 1 February 2006. *BBC*. http://news.bbc.co.uk/2/hi/uk_news/3873323.stm (Accessed 17 July 2014.)

harasses or creates alarm, distress or fear,[90] as well as harassment.[91] **Germany** restricts expression that amounts to Nazi propaganda and Holocaust denial, incitement to hatred (insulting, maliciously maligning, defaming), material causing others to commit a crime and depictions of violence.[92] **China** prohibits ethnic hate speech.[93] In the **United States** hate speech is legal as long as it does not incite 'imminent lawless action' (see above). It is interesting to note that although the EU outlawed Holocaust denial in 2007,[94] member countries have the option of not enforcing the law, which is what the UK did; in contrast it is illegal in Germany and Hungary.[95]

Election-related: In **Kenya,** devastating violence (in which more than 1,000 people died) was partly fuelled by inflammatory text messages circulated after the 2007 Kenyan presidential election.[96] The Communications Commission of Kenya's guidelines for the 2013 election required all bulk political messages to be sent in English or Kiswahili, Kenya's two official languages, and they had to be submitted for approval 48 hours in advance.[97] But these regulations were limited in scope to SMS messages, and the Kenyan government had not implemented precautionary measures on hate speech on Facebook and Twitter, whose Kenyan user bases had skyrocketed since 2007. The National Cohesion and Integration Commission and civil society groups like Umati stepped in to monitor

90 UK Government. 1997. Public Order Act 1986, Sections 4 and 4A. The National Archives. www.legislation.gov.uk/ukpga/1986/64 (Accessed 18 July 2014.)

91 UK Government. 1997. Protection from Harassment Act 1997. The National Archives. www.legislation.gov.uk/ukpga/1997/40/contents (Accessed 18 July 2014.)

92 German Government. *Strafgesetzbuch* [German Criminal Code]. Section 130: Incitement to Hatred. www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1200 and Chapter 14: Libel and Slander. www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1654 (Accessed 18 July 2014); Voluntary Self-Monitoring of Multimedia Service Providers (FSM e. V.). Illegal Content: Youth Protection – What must I know? www.fsm.de/youth-protection/media-content/illegal-content

93 Article 15 of the *Measures on the Administration of Internet Information Services* lists nine categories of content that are prohibited on the internet information service providers. One of these includes content that incites ethnic hatred or racial discrimination or damages inter-ethnic unity. State Council Information Office. 7 June 2012. Measures on the Administration of Internet Information Services (Deliberation Draft). Sina.com. http://news.sina.com.cn/c/2012-06-07/135924552816.shtml (Accessed 17 July 2014.)

94 European Commission. 28 November 2008. Framework Decision on Racism and Xenophobia. http://ec.europa.eu/justice/fundamental-rights/racism-xenophobia/framework-decision/index_en.htm

95 John C. Knechtle. 2008. Holocaust Denial and the Concept of Dignity in the European Union. *Florida State University Law Review*, Vol. 36, pp. 41–66. www.law.fsu.edu/journals/lawreview/downloads/361/knechtle.pdf ; Robert A. Kahn. June 2004. Holocaust Denial and the Law: A Comparative Study. New York, N.Y., Palgrave Macmillan; Dan Bilefsky. 19 April 2007. EU adopts measure outlawing Holocaust denial. New York Times. www.nytimes.com/2007/04/19/world/europe/19iht-eu.4.5359640.html (Accessed 4 August 2014.)

96 Jeffrey Gettleman. 8 February 2008. U.S. Intensifies Efforts to End Deadly Conflict in Kenya. *New York Times*. www.nytimes.com/2008/02/08/world/africa/08kenya.html (Accessed 23 June 2014); Kenya Information and Communication Act, op cit., Section 29.

97 Lucy Purdon. November 2013. *Corporate Responses to Hate Speech in the 2013 Kenyan Presidential Elections. Case Study: Safaricom. Institute for Human Rights and Business. (Digital Dangers: Identifying and Mitigating Threats in the Digital Realm.)* p. 24. www.ihrb.org/pdf/DD-Safaricom-Case-Study.pdf ; Winfred Kagwe. 22 August 2012. Kenya: CCK Draws Up Rules to Curb Hate Speech in Political SMS. *AllAfrica*. http://allafrica.com/stories/201208220319.html (Accessed 23 July 2014.)

hate speech on social media.[98] **Brazil**, where voting is compulsory,[99] prohibits electoral 'propaganda' up to three months prior to elections,[100] while electoral candidates may submit requests for the removal of online content that offends 'dignity or decorum' or points out illegal propaganda. Content providers may be held liable if they do not remove the alleged illegal content once notified.[101] Of similar intent are provisions in the **United Kingdom** that criminalize making a false statement, during an election, about a person standing for office.[102]

Child protection: Child pornography – also known as 'child sexual abuse images' – is illegal in all countries studied.[103] Another category of online content related to child protection involves content that may be legal for adults but is deemed inappropriate for children.[104] The **United Kingdom** bans child sexual abuse images in addition to pornography of various forms.[105] In **Germany**, service providers are prohibited from distributing content that is harmful to young persons, including adult content.[106] In **Russia**, Federal Law No. 139 (the 'blacklist law') allows the government to add websites to a blacklist in order

---

98 Drazen Jorgic. 5 February 2013. Kenya tracks Facebook, Twitter for election 'hate speech'. Reuters. www.reuters.com/article/2013/02/05/net-us-kenya-elections-socialmedia-idUSBRE9140IS20130205 (Accessed 3 August 2014); Mike Pflanz. 21 March 2013. In Kenya, social media hate speech rises as nation awaits election ruling. *The Christian Science Monitor*. www.csmonitor.com/World/Africa/2013/0321/In-Kenya-social-media-hate-speech-rises-as-nation-awaits-election-ruling (Accessed 4 August 2014.)

99 Leticia Calderón-Chelius. 2007. Brazil: compulsory voting and renewed interest among external voters. *Voting from Abroad: The International IDEA Handbook*. Stockholm, International Institute for Democracy and Electoral Assistance and Federal Electoral Institute of Mexico, pp. 128–31. www.idea.int/publications/voting_from_abroad/upload/chap5-brazil.pdf

100 Federal Government of Brazil. 30 September 1997. Presidência da República Casa Civil Subchefia para Assuntos Jurídicos [Brazilian Electoral Law]. Palácio do Planalto, Article 73. (In Portuguese.) www.planalto.gov.br/ccivil_03/leis/l4737.htm (Accessed 1 August 2014.)

101 Federal Government of Brazil. 30 September 1997. Presidência da República Casa Civil Subchefia para Assuntos Jurídicos [Brazilian Electoral Law]. Palácio do Planalto, Articles 57-D, 57-F and 58. (In Portuguese.) www.planalto.gov.br/ccivil_03/leis/l4737.htm; Luciani Gomes. 19 August 2010. Brazilian law way too serious, comics say. CNN. www.cnn.com/2010/WORLD/americas/08/19/brazil.election.comics (Accessed 18 July 2014); Gabriel Elizondo. 25 August 2010. Brazilian elections no joke. Literally. *Al Jazeera*. http://blogs.aljazeera.com/blog/americas/brazilian-elections-no-joke-literally (Accessed 18 July 2014.)

102 UK Government. Representation of the People Act 1983 – Section 106: False statements as to candidates. The National Archives. www.legislation.gov.uk/ukpga/1983/2/section/106

103 However, the United States provides broad immunity for intermediaries and there is no 'affirmative obligation to monitor and screen Web sites for objectionable content, including even child pornography' (though all US companies examined in this report participate in voluntary initiatives to combat child pornography). Legal Information Institute. 18 U.S. Code § 2258A – Reporting requirements of electronic communication service providers and remote computing service providers. Cornell University Law School. www.law.cornell.edu/uscode/text/18/2258A; Roxanne E. Christ, Jeanne S. Berges and Shannon C. Trevino. July 2007. Social Networking Sites: To Monitor or Not to Monitor Users and Their Content? *Intellectual Property and Technology Law Journal*, Vol. 19, No. 7, p. 2, www.lw.com/thoughtLeadership/social-networking-monitoring-content-texas-case

104 Victoria Nash, 2013: Analyzing Freedom of Expression Online: Theoretical, empirical, and normative contributions, in: Dutton, W.H. (eds.) The Oxford Handbook of Internet Studies, Oxford University Press, p. 411-463.

105 UK Government. Criminal Justice and Immigration Act 2008. The National Archives. www.legislation.gov.uk/ukpga/2008/4/part/5/crossheading/pornography-etc; UK Government. Protection of Children Act 1978. The National Archives. www.legislation.gov.uk/ukpga/1978/37

106 Federal Republic of Germany. April 2010. *Kommission für jugendmedienschutz der landesmedienanstalten* (KJM). Interstate Treaty on the protection of minors –JMStV, Section 1, Article 4. www.die-medienanstalten.de/fileadmin/Download/Rechtsgrundlagen/Gesetze_aktuell/_JMStV_Stand_13_RStV_mit_Titel_english.pdf

to protect children from information on the internet such as pornography, drugs and suicide.[107]

Blasphemy: In **India** blasphemous speech, though not defined, is prohibited under the Information Technology Intermediaries Guidelines Rules 2011.[108] The Indian Penal Code does not use the word 'blasphemy' but criminalizes 'deliberate and malicious acts, intended to outrage religious feelings or any class by insulting its religion or religious beliefs'.[109] In **Egypt**, blasphemy is a criminal offence, punishable with up to five years in prison, for anyone who 'makes use of religion in propagating, either by words, in writing, or in any other means, extreme ideas for the purpose of inciting strife, ridiculing or insulting a heavenly religion or a sect following it, or damaging national unity'.[110]

Intellectual property: In **Russia,** according to the new Federal Law No. 187 ('the anti-piracy law') passed in 2013, it is illegal to share content in a manner that violates copyright.[111] In **Brazil**, 'the transmission and retransmission' of content infringing on intellectual property rights can be immediately discontinued or interrupted upon order from a competent judicial authority.[112] In **Germany,** public distribution or duplication of copyrighted material without permission from the rights holder is prohibited although personal and private uses are permitted.[113] In the **United States** copyright is often cited to impose restrictions on online expression, although trademark violations are occasionally cited as well.[114] Details on the application of intellectual property laws to internet intermediaries will be covered in the 'Intermediary Liability' section.

---

107 Once a website is on the registry, content-hosting providers have 24 hours to notify the website owner to remove the prohibited content. The website owner is given another 24 hours to comply. If the website owner fails to take down the banned content, Internet service providers must restrict access to the website within 24 hours. Russian Federation. 28 July 2012. Federal Law No. 139-FZ, on Amending the Federal Law on Protection of Children from Information Harmful to their Health and Development and Other Legislative Acts of the Russian Federation. (In Russian.) www.rg.ru/2012/07/30/zakon-dok.html; President of Russia. 31 July 2012. Amendments to the law on protecting children from information harmful to their health and development. http://eng.kremlin.ru/acts/4246. Sergei Hovyadinov. World Intermediary Liability Map: Russia. Center for Internet and Society at Stanford Law School. http://cyberlaw.stanford.edu/page/wilmap-russia (Accessed 4 August 2014.)

108 Information Technology (Intermediaries Guidelines) Rules, 2011, http://cis-india.org/internet-governance/resources/intermediary-guidelines-rules

109 Pranesh Prakash. 8 April 2012. Section 295A of the Indian Penal Code. Centre for Internet and Society. http://cis-india.org/internet-governance/resources/section-295a-indian-penal-code (Accessed 17 July 2014.)

110 Article 98(f) of the Penal Code, as amended by Law 147/2006. Law 58 of 1937 (Criminal Code of 1937), Art. 98(f). (In Arabic.) www.mohamoon-montada.com/Default.aspx?action=ArabicLaw&ID=20

111 Russian Federation. 2 July 2013. Federal Law No. 187-FZ of July 2, 2013, on Amendments to Certain Legislative Acts of the Russian Federation Concerning the Protection of Intellectual Rights in Information and Telecommunication Networks. World Intellectual Property Organisation. www.wipo.int/wipolex/en/text.jsp?file_id=334516

112 Article 102 and 105 of the Brazilian Copyright Law

113 German Government. 9 September 1965. *Gesetz über Urheberrecht und verwandte Schutzrechte* [Act on Copyright and Related Rights]. English translation. Article 53. www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html

114 Kate Tummarello. 19 December 2013. Google: US government takedown requests up 70 percent. *The Hill*. http://thehill.com/policy/technology/193661-google-us-government-takedown-requests-up-70-percent (Accessed 28 July 2014.)

2.1.2 Privacy, Data Protection, and Surveillance

Privacy and Data Protection: A 2012 report commissioned by UNESCO which covered many of the countries covered in this case study concluded that privacy laws or legal provisions that provide only weak protection can have a negative impact on freedom of expression.[115] A significant number of human rights groups lauded the passage of European Parliament's passage in March 2014 of the new General Data Protection Regulation,[116] which places greater privacy requirements on internet intermediaries operating in Europe.[117] Efforts elsewhere around the world vary. The United States lacks comprehensive consumer data protection legislation, relying instead on a patchwork of federal and state laws.[118] While Brazil does not have a general data protection law or framework as of September 2014, Marco Civil da Internet includes data protection provisions.[119] The Kenyan parliament at the time of writing was considering a data protection bill.[120] India, at the time of writing, does not have comprehensive privacy legislation, though data protection standards applicable to corporate and digital information can be found under section 43A of the Information Technology Act 2000 and subsequent Rules.[121]

At the same time, many actors seek to curtail the expression of some citizens to protect the privacy of others. This is of contemporary significance in the **European Union** given the case of *Google Spain v AEPD,* described in shorthand as establishing a 'right to be forgotten' throughout the EU. It will be discussed in more detail in Study 2, which focuses

115 Mendel, et. al. op. cit. pp. 95–96.

116 Stephen Gardner. 17 March 2014. European Parliament Votes Overwhelmingly In Favor of Data Protection Reform Proposal. *Bloomberg BNA Privacy & Security Law Report*. www.bna.com/european-parliament-votes-n17179885695 (Accessed 28 July 2014); David Jolly. 13 March 2014. European Union Takes Steps Toward Protecting Data. *New York Times*. www.nytimes.com/2014/03/13/business/international/european-union-takes-steps-toward-protecting-data.html (Accessed 28 July 2014.)

117 Marc Rotenberg and David Jacobs. 2013. Updating the Law of Information Privacy: The New Framework of the European Union. *Harvard Journal of Law & Public Policy*, Vol. 36, No. 2, pp. 605–52. www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_605_Rotenberg_Jacobs.pdf; Nina Haase. 11 March 2014. EU Parliament approves privacy package. *Deutsche Welle*. www.dw.de/eu-parliament-approves-privacy-package/a-17488815 (Accessed 17 July 2014.)

118 Natasha Singer. An American Quilt of Privacy Laws, Incomplete. The New York Times. 30 March 2013. http://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html (Accessed 17 July 2014.)

119 Knowledge Commons Brasil. Statement on Data Retention Provisions in Marco Civil. http://www.knowledgecommons.in/brasil/en/marco-civil/statement-on-data-retention-provisions-in-marco-civil/ (Accessed 17 July 2014.) and Chris Riley. Marco Civil – A groundbreaking, although not perfect, victory for Brazilian Internet Users. Mozilla Open Policy & Advocacy. 25 March 2014 https://blog.mozilla.org/netpolicy/2014/03/26/marco-civil-a-groundbreaking-although-not-perfect-victory-for-brazilian-internet-users/ (Accessed 17 July 2014.)

120 Commission for the Implementation of the Constitution. The Data Protection Bill, 2012. http://www.cickenya.org/index.php/legislation/item/174-the-data-protection-bill-2012#.VC_6Z-enYbB

121 Section 43A of the Information Technology Act 2000 as amended in 2008, available at: http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf The Information Technology Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011. Available at: http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

on search engines.[122] The decision demonstrates that the individual's desire to eliminate negative information about him- or herself from the internet can be in direct conflict with the right of others to receive and impart information.[123]

Surveillance and government access to user data: The UN High Commissioner for Human Rights has called for reform of surveillance laws, and referred to the recommendations by global civil society for the application of the 'necessary and proportionate' principles with strong accountability, transparency, and remedy.[124] However, a recent survey of experts in 18 countries showed that little surveillance reform has taken place around the world.[125] In many places new laws have continued to expand government surveillance powers: Most recently in July 2014 the **United Kingdom** enacted a new law, the Data Retention and Investigatory Powers Act, extending government surveillance powers beyond the UK's borders[126] by allowing government to issue warrants for the interception of communications to companies outside of the UK.[127] Similarly, **Brazil**'s Marco Civil da Internet empowers authorities to access data stored abroad if the intermediary provides services to or collects data from Brazilian citizens.[128] In **Russia**, it appears that opposition activists and protest groups may be monitored via domestic intermediaries: Pavel Durov, founder and former CEO of VKontakte, Russia's most popular social network with 60 million users,[129] claims to have spurned a Russian security agency request for the private user data of belonging to members of several Ukrainian protest groups.[130]

Surveillance has been documented to have an impact on freedom of expression in a range of jurisdictions. For example, in the **United States**, in the wake of revelations about the

---

122 Court of Justice of the European Union. Case C-434/09. 13 May 2014. *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*. EU:C:2014:317. http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN

123 Global Network Initiative. 15 May 2014. EU Court 'Right to Be Forgotten' Ruling Threatens Freedom of Expression. www.globalnetworkinitiative.org/news/eu-court-%E2%80%98right-be-forgotten%E2%80%99-ruling-threatens-freedom-expression (Accessed 17 July 2014.)

124 Pillay, op. cit.; Necessary and Proportionate. 10 July 2013. International Principles on the Application of Human Rights to Communications Surveillance. https://en.necessaryandproportionate.org/text.

125 Simon Davies (ed). June 2014. A Crisis of Accountability: A global analysis of the impact of the Snowden revelations. *Privacy Surgeon*. www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf

126 Jemima Kiss. 15 July 2014. Academics: UK 'Drip' data law changes are 'serious expansion of surveillance'. *The Guardian*. www.theguardian.com/technology/2014/jul/15/academics-uk-data-law-surveillance-bill-rushed-parliament (Accessed 16 July 2014.)

127 Jemima Kiss. Op. cit.; Data Retention and Investigatory Powers Act 2014 Chapter 27. Pg. 8, Sec.4(2). http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf

128 Marco Civil da Internet. Article 11 section 2. http://sflc.in/wp-content/uploads/2014/05/APPROVED-MARCO-CIVIL-MAY-2014.pdf

129 As of December 2013, according to comScore, Facebook was in third place with 7.8 million Russian users and behind Odnoklassniki, a school-based Russian social network with 54 million Russian users. Kathrin Hille. 26 January 2014. VKontakte stake sale strengthens Usmanov grip. *Financial Times*. www.ft.com/cms/s/0/25037bce-867c-11e3-aa31-00144feab7de.html (Accessed 1 August 2014.)

130 Carol Matlack. 17 April 2014. The Kremlin Tried to Use VKontakte—Russia's Facebook—to Spy on Ukrainians. *Bloomberg Businessweek*. www.businessweek.com/articles/2014-04-17/the-kremlin-tried-to-use-vkontakte-russias-facebook-to-spy-on-ukrainians (Accessed 1 August 2014); Liga Business Inform. 18 April 2014. Большой брат: как соцсети делятся информацией со спецслужбами [Big brother: How social networks share information with security services]. Liga Business Inform. (In Russian.) http://biz.liga.net/print/all/it/stati/2732697-bolshoy-brat-kak-sotsialnye-seti-slivayut-dannye-spetssluzhbam.htm (Accessed 17 July 2014.)

apparent scale of the NSA's surveillance, the PEN American Center conducted a survey of over 520 American writers about the effects of surveillance on their work. The report noted that 16 per cent claimed to 'have refrained from conducting Internet searches or visiting Web sites on topics that may be considered controversial or suspicious, and another 12 per cent have seriously considered it'.[131]

The European Union faces a growing disconnect between surveillance powers sought by governments and what courts view as necessary and proportionate. In April 2014 the European Court of Justice (ECJ) ruled that the EU Data Retention Directive was invalid[132] and contained provisions that disproportionally interfered with 'the private lives of citizens'.[133] The UK Government instructed ISPs to continue to retain data despite the ECJ ruling.[134] It then invoked 'emergency measures' to expedite passage of the Data Retention and Investigatory Powers Act,[135] effectively overriding the ECJ decision by requiring ISPs to continue storing metadata for one year.[136] Government officials were quoted in news reports noting that the legislation was necessary to maintain the 'tools' needed to combat terrorism and to ensure public safety. The UK has not been the only country in Europe to disagree with the ECJ ruling; Austria, Belgium, Bulgaria, Germany, Greece, Romania and Sweden have also rejected it.[137]

2.2 Intermediary liability

What happens when an internet user uses an intermediary service to post, share, or access content that infringes laws in a given country? To what extent can or should intermediaries be held legally responsible – or "liable" – for the activities of their users? This question is answered by a regulatory approach most commonly around the world as "intermediary liability."

Intermediary liability provisions formalize government expectations for how an intermediary must handle 'third-party' content or communications. In some intermediary liability approaches, such legal provisions define circumstances under which intermediaries can be exempt from liability by setting forth criteria that intermediaries must follow in order to escape civil or even sometimes criminal penalty for users' actions.

---

131 PEN American Center. 12 November 2013. Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor. www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

132 Danny O'Brien. Data Retention Directive Invalid, says EU's Highest Court. 8 April 2014. https://www.eff.org/deeplinks/2014/04/data-retention-violates-human-rights-says-eus-highest-court (Accessed 17 July 2014.)

133 Court of Justice of the European Union PRESS RELEASE No 54/14 Luxembourg, 8 April 2014. Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

134 Pam Cowburn. DRIP: Five Arguments Against Proposed UK Data Retention Bill. London School of Economics and Political Science Media Policy Project Blog. 15 July 2014. (Accessed 1 August 2014.) http://blogs.lse.ac.uk/mediapolicyproject/2014/07/15/drip-five-arguments-against-proposed-uk-data-retention-bill/

135 Parliament passes emergency Data Retention Bill. BBC News. 17 July, 2014. http://www.bbc.com/news/uk-politics-28352673 (Accessed 1 August 2014.)

136 Dave Lee. What emergency data law means for you. 10 July 2014. http://www.bbc.com/news/technology-28245589 (Accessed 1 August 2014.)

137 Cowburn, op. cit.

2.2.1 Models of Intermediary Liability

Many governments in regions including Europe, North America, parts of South East Asia and Latin America, have laws specifically addressing intermediary liability. In other regions, particularly Africa, governments are considering legal provisions on intermediary liability.[138] Broadly speaking, where such regimes exist, there are three models of intermediary liability:[139] which strict liability, conditional liability and broad immunity.[140] Exact requirements and nuances of these models vary from jurisdiction to jurisdiction, and are defined by governments and further clarified by courts. Some intermediaries explicitly comply with legal mandates relating to intermediary liability by undertaking measures such as self-regulation via enforcement of their terms of service.

'Blanket' or strict liability: The intermediary is liable for third-party content even when it is not aware that the content is illegal (or even exists). The only way to avoid liability under such circumstances is to monitor, filter, and remove content proactively if it is likely to be infringing. Even so, monitoring and removing content does not absolve the intermediary of liability if any infringing content is overlooked. Blanket liability regimes do not distinguish between intermediaries; all intermediaries, regardless of size or function, are liable. China and Thailand are governed by strict liability regimes.[141] For example the Chinese government imposes liability for unlawful content on all intermediaries. If they fail to sufficiently monitor user activity, take down content or report violations, they may face fines, criminal liability, and revocation of business or media licenses.[142] In 2014 the leading portal, Sina.com, had part of its publishing licenses revoked due to the presence of pornographic material on its network.[143]

'Safe harbour' or conditional liability: The intermediary is potentially exempt from liability for third-party content if certain conditions are met – such as removing content upon receiving notice ('notice and takedown'), notifying the content creator of infringing material after receiving notice ('notice and notice') or disconnecting repeat infringers

138 Elimar Vushe Gandhi. 19 May 2014. Internet Intermediaries: The dilemma of liability in Africa. *Association for Progressive Communications News*. www.apc.org/en/node/19279 (Accessed 17 July 2014.)

139 For more information about the different intermediary models, see Article 19, 'Dilemma', p. 7; Center for Democracy and Technology, op. cit., p. 4.

140 For more information about the different intermediary models, see Article 19, 'Dilemma', p. 7; Center for Democracy and Technology, op. cit., p. 4.

141 Center for Democracy and Technology, op. cit., pp 14-16.

142 Measures for Managing Internet Information Services, Article 20 [in Chinese], issued by the State Council on September 25, 2000, effective October 1, 2000. Unofficial English translation available at http://www.chinaculture.org/gb/en_aboutchina/2003-09/24/content_23369.htm. See also OpenNet Initiative, Access Contested, MIT Press, 2011, http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf, pp. 279–80.

143 Glyn Moody. 30 April 2014. China's Internet Giant Sina.com Loses Publication License for Publishing Pornography – 20 Articles and Four Videos. *Techdirt*. www.techdirt.com/articles/20140425/09451027029/chinas-internet-giant-sinacom-loses-publication-license-publishing-pornography-20-articles-four-videos.shtml (Accessed 17 July 2014.)

upon notice.[144] If an intermediary does not meet these stipulations, they may be liable for damages.145 Unlike the 'strict liability' model, the safe harbour model does not compel intermediaries to proactively monitor and filter content in order to avoid liability.[146] However, there are a wide variety of safe harbour regimes; for example, the EU E-Commerce Directive (ECD) establishes criteria under which different categories of intermediaries can seek exemption from liability,[147] whereas South Africa's Electronic Communications and Transactions Act[148] only recognizes safe harbour for the 169 member companies[149] that belong to the Internet Service Providers' Association, South Africa's self-regulatory industry group.[150]

The 'notice-and-takedown' variety of conditional liability – such as the United States' Digital Millennium Copyright Act (DMCA) – is criticized because it is easy to abuse; furthermore, it facilitates self-censorship by placing the intermediary in a quasi-judicial position responsible for evaluating the legality of content.[151] The model is even more susceptible to abuse when it lacks elements of due process, such as the opportunity to appeal a takedown request.[152] Indeed, 'notice-and-takedown' incentivizes intermediaries to remove content immediately after receiving notice, rather than investing resources to

144 The OECD identified four ways in which intermediaries cooperate with law enforcement: (a) Notice and takedown; (b) Notice and notice; (c) Notice and disconnection; and (d) Filtering. Organisation for Economic Co-operation and Development. September 2011. *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. Paris, OECD Publishing, pp. 143–162. http://browse.oecdbookshop.org/oecd/pdfs/product/9311031e.pdf

145 Center for Democracy and Technology, op. cit.

146 Article 19, op. cit., p. 7.

147 European Parliament and the Council of the European Union. 8 June 2000. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). EUR-Lex. Articles 12, 13, and 14. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML

148 Republic of South Africa. 31 July 2002. Electronic Communications and Transactions Act, 2002 (No. 25 of 2002.) www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislations/South%20Africa/ElecComm.PDF

149 List of members. South Africa, Internet Service Providers' Association. http://ispa.org.za/membership/list-of-members

150 Republic of South Africa. 31 July 2002. Electronic Communications and Transactions Act, 2002 op. cit. List of members. South Africa, Internet Service Providers' Association. op. cit.; Alex Comninos and Andrew Rens. Alex Comninos and Andrew Rens. 19 May 2014. Intermediary Liability: New Developments in South Africa. *Association for Progressive Communications News*. www.apc.org/en/node/19204 (Accessed 17 July 2014); Republic of South Africa. 31 July 2002. Electronic Communications and Transactions Act. WILMap. (Act N. 25/2002.) https://cyberlaw.stanford.edu/page/wilmap-south-africa (Accessed 31 July 2014.)

151 Wendy Seltzer. Fall 2010. Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment. *Harvard Journal of Law & Technology*, Vol. 24, No. 1, pp. 171–232. http://jolt.law.harvard.edu/articles/pdf/v24/24HarvJLTech171.pdf

152 Carolina Rossini and Maira Sutton. *The Impact of Trade Agreements on Innovation, Freedom of Expression and Privacy: Internet Service Providers' Safe Harbors and Liability*. San Francisco, Electronic Frontier Foundation. https://www.eff.org/files/filenode/ISPLiability_FNL.pdf

investigate the validity of the request and risk a lawsuit. Legitimate content can end up being censored as a consequence.[153]

A 2011 study on India's intermediary liability regime by the Centre for Internet and Society in Bangalore indicated a need for increased safeguards against misuse of the privately administered takedown regime. Specifically, the study identified a need to: reduce uncertainty in the criteria for administering takedowns; reduce uncertainty in the procedure for administering takedowns; include various elements of natural justice (prevention of bias and emphasis on the right to a fair hearing) in the procedure for administering takedowns; and replace the requirement for subjective legal determination by intermediaries with an objective test.[154] These issues have been echoed in jurisdictions such as South Africa, particularly with respect to the lack of due process for users whose content is removed.[155]

Broad immunity: In this model the intermediary is exempt from liability for a range of third-party content without distinguishing between intermediary function and content type.[156] For example, section 230 of the Communications Decency Act in the USA shields intermediaries from liability for illegal behaviour by users while also protecting them from liability when they do remove content in compliance with private company policy.[157] Exceptions to this model include intellectual property (copyright is governed by the Digital Millennium Copyright Act, trademark by the Lanham Act), and US federal criminal law.[158]

Given the key role that intermediaries and the laws that govern them play in online freedom of expression, discussions at the international level have sought to establish common principles and best practices. For example, in December 2011, the OECD Council included 'limiting intermediary liability' as one of 14 recommended principles for internet policy-making to 'promote and protect the global free flow of information online'. These principles also emphasized the importance of transparency, due process, accountability

153 For an egregious example of 'notice and takedown' as an instrument of taking down legal content, see Paul Sieminski. 21 November 2013. Striking Back Against Censorship. WordPress Hot Off the Press Blog. http://en.blog.wordpress.com/2013/11/21/striking-back-against-censorship (Accessed 17 July 2014); Corynne McSherry. 21 November 2013. WordPress.com Stands Up For Its Users, Goes to Court to Challenge DMCA Abuse. EFF Deeplinks Blog. https://www.eff.org/deeplinks/2013/11/wordpresscom-stands-its-users-goes-court-challenge-dmca-abuse (Accessed July 2014); Mike Masnick. 21 November 2013. Wordpress Goes Legal: Sues Over Two Egregiously Bogus DMCA Notices That Were Designed To Censor. Techdirt. www.techdirt.com/articles/20131121/01431725317/wordpress-goes-legal-sues-over-two-egregiously-bogus-dmca-notices-that-were-designed-to-censor.shtml (Accessed 17 July 2014.)

154 Rishabh Dara. 2011. *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*. The Centre for Internet and Society, p. 2. http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf (Accessed 17 July 2014.)

155 Comninos and Rens, op. cit.

156 Article 19, 'Dilemma', op. cit., p. 7.

157 Legal Information Institute. 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material. Cornell University Law School. www.law.cornell.edu/uscode/text/47/230 (Accessed 18 July 2014.)

158 Center for Democracy and Technology, op. cit., p. 4.

and inclusive, multistakeholder policymaking.[159] An advisory council comprised of civil society groups endorsed the recommendation.[160]

2.2.2 Intermediary Liability in the Case Study Countries

Intermediary liability policy appears to be evolving into a legal mechanism that, in part, allows governments to transpose their own interpretations of limitations to freedom of expression onto the internet. Depending on the national, social and historical context, different governments emphasize the restriction of different types of content as outlined in section 2.1 above.[161]

For example, cyber cafes attract particular regulation in India,[162] while telecommunication companies and the potential spread of hate speech via SMS services are a strong concern in Kenya.[163] Depending on the jurisdiction, non-compliant intermediaries may face criminal prosecution like imprisonment, civil penalties like fines or a revocation of operating licenses. Below are brief summaries of the intermediary liability regimes of the case study countries plus the European Union of which three of those countries are members.[164]

159 Organisation for Economic Co-operation and Development. 13 December 2011. *OECD Council Recommendation on Principles for Internet Policy Making*. www.oecd.org/internet/ieconomy/49258588.pdf

160 Civil Society Information Society Advisory Council. 18 December 2011. 'CSISAC Welcomes OECD Recommendation on Principles for Internet Policy Making'. http://csisac.org/2011/12/oecd_principles_internet_policy.php

161 For more detailed analysis of intermediary liability regimes in these and other countries see the Center for Internet and Society at Stanford Law School's World Intermediary Liability Map (WILMap) project at https://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap

162 India recognizes Cyber Cafes as intermediaries and has created explicit Rules for Cyber Cafes under the Information Technology Act 2000. Among other things, the rules require Cyber Cafes to (a) register all users of the facilities with photo identification, (b) record and store user browser history for one year, and (c) cooperate with authorities when required. Nikhil Pahwa. 2 May 2011. India's CyberCafe Rules Finalized; Foundation For Harassment. *MediaNama*. www.medianama.com/2011/05/223-india-cyber-cafe-law (Accessed 17 July 2014); Bhairav Acharya. 31 March 2013. Comments on the Information Technology (Guidelines for Cyber Cafe) Rules, 2011. The Centre for Internet and Society. http://cis-india.org/internet-governance/blog/comments-on-the-it-guidelines-for-cyber-cafe-rules-2011; Department of Electronics and Information Technology, Ministry of Communications and IT, Government of India. 11 April 2011. Information Technology (Guidelines for Cyber Cafe) Rules, 2011. GSR 315(E). http://deity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf

163 Comninos, An Uncertain Terrain, op. cit., p. 10.

164 Center for Internet and Society at Stanford Law School, World Intermediary Liability Map, op. cit.

Brazil: On 23 April 2014, Brazilian President Dilma Rousseff signed the Marco Civil da Internet into law,[165] Brazil's first law addressing intermediary liability.[166] Intermediaries qualify for safe harbor as long as they remove third-party content after receiving a court order.167 Failure to comply with a court order can result in arrest, as it did in 2012 when the Brazilian electoral court issued warrants for the arrest of two Google executives for not removing a film that made negative remarks about a local mayoral candidate in violation of a 1965 Brazilian electoral law before the 2012 elections.[168]

The Marco Civil leaves issues related to copyrighted content[169] and electoral propaganda[170] to specific legislation. Cases related to violations of honour and reputation or personality rights may be heard by Small Claims Courts, which provides a more expedited process.[171] The one exception to the safe harbour provisions is when 'revenge porn' is involved; Article 21 of Marco Civil states that intermediaries may be secondarily liable if they do not remove content that depicts 'disclosure, without consent of its participants, of photos, videos or other materials containing nudity or acts sexual private character, after receipt of notification by the participant or legal representative'.[172] If a service provider has the contact information of the user who published the content, they must notify the users of the reasons and other information related to the removal.[173]

China: In Chinese legal terms, the concept of internet intermediaries is encapsulated by the concept of 'Internet Information Service' as outlined in Article 2 of the Measures on the Administration of Internet Information Services (Measures).[174] According to Article

165 Anthony Boadle. 23 April 2014. Brazilian Congress passes Internet bill of rights. Reuters. www.reuters.com/article/2014/04/23/us-internet-brazil-idUSBREA3M00Y20140423 (Accessed 17 July 2014); Daniel P. Cooper. 28 April 2014. Brazil Enacts 'Marco Civil' Internet Civil Rights Bill. Covington & Burling LLP. www.natlawreview.com/article/brazil-enacts-marco-civil-internet-civil-rights-bill (Accessed 17 July 2014.)

166 Anthony Boadle. 23 April 2014. Brazilian Congress passes Internet bill of rights. *Reuters*. (Accessed 17 July 2014); Daniel P. Cooper. 28 April 2014. Brazil Enacts 'Marco Civil' Internet Civil Rights Bill. Covington & Burling LLP. (Accessed 17 July 2014.); Diego Spinola. Diego Spinola. 30 April 2014. Brazil Leads the Efforts in Internet Governance with Its Recently Enacted 'Marco Civil Da Internet'. What's In It For Intermediary Liability? Center for Internet and Society at Stanford Law School. http://cyberlaw.stanford.edu/blog/2014/04/brazil-leads-efforts-internet-governance-its-recently-enacted-marco-civil-da-internet (Accessed 31 July 2014.)

167 Federative Republic of Brazil. 23 April 2014. Marco Civil da Internet, Law No. 12.965 Article 19. http://sflc.in/wp-content/uploads/2014/05/APPROVED-MARCO-CIVIL-MAY-2014.pdf

168 Sarah Laskow. 29 April 2013. Google vs Brazil. *Columbia Journalism Review*. www.cjr.org/cloud_control/brazilian_takedown_requests.php?page=all (Accessed 18 July 2014); Sorcha Pollack. 27 September 2012. Google Executive Arrested as Brazil Bans Anti-Muslim Film. *Time*. http://newsfeed.time.com/2012/09/27/google-executive-arrested-as-brazil-bans-anti-muslim-film (Accessed 18 May 2014); Larissa G. Alfonso, Felipe Octaviano Delgado Busnello, and Diego C. Spinola. World Intermediary Liability Map: Brazil. Center for Internet and Society at Stanford Law School. https://cyberlaw.stanford.edu/page/wilmap-brazil (Accessed 30 July 2014.)

169 Marco Civil da Internet, op. cit., Article 31.

170 Federal government of Brazil. 30 September 1997. Presidência da República Casa Civil Subchefia para Assuntos Jurídicos [Brazilian Electoral Law]. Palácio do Planalto, Article 57-F. (In Portuguese.) www.planalto.gov.br/ccivil_03/LEIS/L9504.htm (Accessed 1 August 2014.)

171 Marco Civil da Internet, op. cit. Article 19(3).

172 Marco Civil da Internet, op. cit. Articles 19 and 21; Pedro Ekman and Bia Barbosa. 27 March 2014. Marco Civil Aprovado: Dia Histórico para Liberdade de Expressão. *Intervozes*. (In Portuguese.) http://intervozes.org.br/marco-civil-aprovado-dia-historico-para-a-liberdade-de-expressao (Accessed 17 July 2014.)

173 Marco Civil da Internet, op. cit., Article 20.

174 State Council Information Office. 7 June 2012. Measures. Op. cit.

13 of the Measures, all 'information service providers" are required to 'ensure that the information that they provide is lawful'. A revised 'deliberation draft' of the Measures was jointly released by the State Information Office and Ministry of Industry and Information Technology in 2012, proposing a number of updated provisions specifying the obligations of ISPs.[175] The draft which is expected to become law and which has therefore already begun to influence company behaviour, stipulates that once an internet information service discovers that the information published falls into the 'nine forbidden content categories', it shall 'immediately stop the publication and transmission thereof, save the relevant records and make a report thereon to the relevant authority and the public security department' (Articles 18 and 19).[176] Article 25 stipulates the creation of a complaints system enabling any member of the public to report illegal content that they see on information service providers to the public security bureau and other relevant government departments.[177]

Egypt: Although Egypt does not have a specific legal regime for intermediary liability, there are laws that have been interpreted as affecting intermediaries. For example, Article 147 of Egypt's 2002 Protection of Intellectual Property Rights Law specifically includes 'computers, internet, information networks, communication networks' among the entities that must respect copyright.[178] On the one hand, Article 147's breadth – which covers 'any manner of' copyright exploitation – may hold intermediaries liable, although another article of the same law, Article 171(9),[179] could be interpreted as a statutory safe harbour indemnifying internet intermediaries in Egypt.[180] Scholars saw support for the latter position in the Egyptian State Council Administrative Court's November 2010 decision to overturn the National Telecommunications Regulatory Authority (NTRA)'s decision to require mobile operators and satellite broadcast companies to monitor their users' news feeds.[181] The NTRA, which is empowered by the Telecommunications Regulatory Law to set rules for telecommunications services providers, requires telecommunications companies (which includes ISPs) to comply with restriction orders[182] from the government or risk imprisonment or revocation of their operating licenses.[183] The Egyptian State

175 Ibid.
176 Ibid.
177 Ibid.
178 Egyptian Gazette. 2 June 2002. Protection of Intellectual Property Rights Law No. 82/2002. World Intellectual Property Organization, p. 47. www.wipo.int/edocs/lexdocs/laws/en/eg/eg001en.pdf (Accessed 18 July 2014.)
179 'Without prejudice to the moral rights of the author under this Law, the author may not, after the publication of the work, prevent third parties from…Ephemeral reproduction of a work where such reproduction is made in relay, during a digital transmission of the work or in the course of a process of reception of a digitally stored work, within the normal operation of the device used by an authorized person.' Egyptian Gazette, pp. 52–53.
180 Seng and Fernandez-Diez, op. cit., pp. 24–25.
181 Yasmine Saleh. 27 November 2010. Egypt's court overturns telecom news monitoring. *Reuters*. www.reuters.com/article/2010/11/27/us-egypt-media-court-idUSTRE6AQ12V20101127 (Accessed 18 July 2014.)
182 National Telecommunication Regulatory Authority of Egypt. February 2003. Egypt Telecommunication Regulation Law, Law No. 10 of 2003. University of Minnesota, p. 26 (Article 67). www1.umn.edu/humanrts/research/Egypt/Egypt%20Telecommunication%20Regulation%20Law.pdf
183 Egypt Telecommunication Regulation Law, op. cit., p. 31 (Article 82.)

Council has the power to issue orders to block or remove content.[184] In brief, there is no consensus on whether the 2002 law 'explicitly impose[s] liability on intermediaries for acts of infringement by third parties or absolve[s] them'.[185]

Germany: In Germany, provisions addressing intermediary liability are defined in the Telemedia Act 2007.[186] The Telemedia Act applies to all electronic information and communication services, excluding broadcasters and telecommunications service providers that consist entirely of the transmission of signals. Telecommunications Services are mainly regulated by the Telecommunications Act.[187] The Telemedia Act established a tiered liability regime that factors in a user's level of involvement in the infringement on the internet; individual 'content providers' are liable for own content they produce, share, post etc. on intermediary platforms. 'Host providers', like social networking platforms, are granted limited liability for third-party content, while 'access providers', or ISPs, are assigned only very limited liability for third-party content.[188] In Germany, a number of state and non-governmental actors can issue requests for filtering, and removal of information.[189]

Hungary: The concept of internet intermediaries was established via Act CVIII of 2001 ('on certain issues of electronic commerce services and information society services'), which implemented the EU E-Commerce Directive (ECD) of 2000.[190] According to the ECD, intermediary service providers are not responsible for the content they transmit, as long as they do not select or modify the information transmitted/stored, specify the recipient and initiate the information (art. 8, par. 1). Furthermore, intermediary service providers are not liable if they have no knowledge of the unlawful nature of the transmitted information and if, having acquired knowledge about its unlawful nature, they act 'expeditiously to remove or to disable access to the information' (art. 11). As the original formulation of Act CVIII refers mostly to copyright infringements, it is unclear how newly enacted restrictions on media content and the modified provisions of the criminal code will impact the legal

184 As an example of an order from a High Administrative Court includes in 2013 a ruling from the High Administrative Court that ordered YouTube to be blocked for a month in the country after Google refused to delete the film 'Innocence of Muslims'. Joel Gulhane. 19 February 2013. Google blocks YouTube videos in Egypt. *Daily News Egypt*. www.dailynewsegypt.com/2013/02/19/google-blocks-youtube-video (Accessed 17 July 2014.)

185 Seng and Fernandez-Diez, op. cit., pp. 24–25.

186 26 February 2007. ***Telemediengesetz*** (TMG) [Telemedia Act (TMA)]. Centre for German Legal Information (CGerLI). Part 3, Sections 7–10. (Federal Gazette I, p. 179), pp. 6–8. www.cgerli.org/fileadmin/user_upload/interne_Dokumente/Legislation/Telemedia_Act__TMA_.pdf

187 CGerLI, op. cit., p. 2; Telecommunications Act, §3, www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html#BJNR119000004BJNG000100000

188 CGerLI, op. cit., pp. 6–8.

189 Government bodies include child protection authorities, Commission for Youth Protection Relating to Media, the Ministry of Interior and the Federal and Criminal Police Office; non-governmental organizations include the Association for the Voluntary Self-Monitoring of Multimedia Service Providers (FSM e.V.), and copyright holders and their representatives.

190 National Media and Infocommunications Authority of Hungary. 24 December 2001. Act CVIII of 2001 on certain issues of electronic commerce services and information society services. http://english.nmhh.hu/dokumentum/150094/108_2001_el_comm_torv_20070502.pdf

situation of intermediary services.[191] Additionally, according to the revised Criminal Code, article 77, content of criminal nature 'disclosed through an electronic communications network' can be ordered by courts to be 'rendered irreversibly inaccessible'.[192]

India: Section 79 of the Information Technology Act 2000 limits the liability of intermediaries for third party information on their networks. Intermediaries are granted exemption from liability for third-party content as long as they do not initiate the transmission, specify its recipient, select or modify the communication and perform due diligence as defined by Rules under section 79.[193] Among other requirements, according to the Rules, the intermediary must work to respond to requests for the removal of information that is in contravention of the Rules within 36 hours of receiving such a request.[194] This safe harbour does not apply if the intermediary has conspired or aided in the commission of the unlawful act, does not expeditiously remove or disable access to the content after receiving notice or has obtained actual knowledge of the infringing content.[195]

Kenya: Kenyan law does not explicitly address the liability of internet intermediaries. The lack of comprehensive regulations around intermediary liability has caused uncertainty in the legal definition and recognition of an 'intermediary', with the closest definition being found in the Kenya Information Communications Act under 'telecommunication operator' or 'licensee'.[196] Internet companies such as social networks and search engines are not defined and therefore do not fall under this definition. Bodies that are authorized to request content removal include the National Cohesion and Integration Commission,[197] the Ministry of Information Communication and Technology,[198] Communication Authority of Kenya[199] and the Kenya Copyright Board.[200] Because of the lack of specific regulation addressing intermediary liability in Kenya, intermediaries can potentially be held liable for illegal content under a number of different laws as mentioned above under 'restrictions'.

---

191 Katalin Parti and Luisa Marin. 2013. Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A Comparative Analysis on Blocking Measures and Internet Providers' Removal of Illegal Internet Content. *Journal of Contemporary European Research*, Vol. 9, No. 1, pp. 138–59. www.jcer.net/index.php/jcer/article/view/455/392

192 Act LXXVIII of 2013. (In Hungarian.) www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13096.pdf

193 Section 79(2) of the Information Technology Act 2000 as amended in 2005 http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

194 Rule 3(4) of the Information Technology Intermediaries Guidelines Rules 2011. Rule 3(2) contains more than thirty-six types of prohibited content. For full list of prohibited content see Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India. 11 April 2011. (1330 GI/11-3A) http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf

195 Section 79 (3) of the Information Technology Act 2000 as amended in 2008, op. cit.

196 Republic of Kenya. 2012. Kenya Information and Communications Act, Section 2. National Council for Law Reporting. www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%20411A#part_II

197 Republic of Kenya. 2008. National Cohesion and Integration Act, No. 12 of 2008. National Council for Law Reporting, p. 17 (Section 25(2)). http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/NationalCohesionandIntegrationAct_No12of2008.pdf

198 Kenya Information and Communications Act, op. cit., Section 5A.

199 Kenya Information and Communications Act, op. cit., Section 5; Communications Authority of Kenya. What we Do. www.ca.go.ke/index.php/what-we-do (Accessed 1 July 2014.)

200 Alice Munyua, Grace Githaiga and Victor Kapiyo. 2012. Intermediary Liability in Kenya. Kenya ICT Action Network, p. 10. www.apc.org/en/system/files/Intermediary_Liability_in_Kenya.pdf (Accessed 1 August 2014.)

Liability can also arise under common law for breach of privacy, negligence, breach of contract, copyright infringement, defamation, vicarious liability, etc.[201] Pertaining specifically to ISPs and telecommunications service providers, under the Kenya Information Communications Act the industry regulator, the Communications Authority of Kenya has general powers to regulate the operations of licensees through, among others, the prescription of rules and conditions for licences. This includes the power to revoke licences for non-compliance with the rules, or the licence terms and conditions.[202]

Russia: In 2013 the 'Anti-piracy law' (Federal Law No. 187-FZ) implemented a number of legal revisions affecting internet intermediaries, including for the first time in Russia's legal code a definition of 'information intermediaries'.[203] The law defines functions performed by different types of 'information intermediaries' – those transferring content through information communication networks including the internet, those providing opportunity to place content or information needed to receive the content, and those providing access to content.[204] It also outlines how these actions can avoid liability for intellectual property right infringement, including by 'safe harbour actions' (depending on the type of intermediary), for example by: 1) not initiating transmission of content nor determining the receiver of the content; and 2) not modifying the content while providing services, save for the changes necessary by the technical process of transmission. It also contained more ambiguous safe harbour requirements such as prompt action to stop infringement upon notification by rights-holders, and knowledge standards about 'ought to know' that the content in question was unlawful.[205] According to recently updated laws governing online content, intermediaries are required to block or take down content upon receiving an order from Roskomnadzor, Russia's communications regulator responsible for overseeing media and internet content.[206] The penalty for failure to delete or block the requested content is significant. Entire websites can be blocked, including the ones which have the similar IP addresses.[207] A February 2014 amendment requires that intermediaries

201 Republic of Kenya. 2007. Chapter 8: The Judicature Act. National Council for Law Reporting, pp. 3–4 (Section 3). www.kenyalaw.org/Downloads/GreyBook/3.%20Judicature%20Act.pdf

202 Section 25, Kenya Information and Communication Act, op. cit.

203 Government of Russia. Article 1253.1 – On responsibility of Informational intermediaries (Civil code of Russian Federation Chapter 69). (In Russian.) www.zakonrf.info/gk/1253.1 (Accessed 18 July 2014); Daria Kim. 24 July 2013. Russia Adopts Measures Against Online Video Piracy. *Intellectual Property Watch*. www.ip-watch.org/2013/07/24/russia-adopts-measures-against-online-video-piracy (Accessed 16 July 2014.)

204 The full name of the law is 'On Amending Separate Legislative Acts of the Russian Federation Concerning the Questions of Protection of Intellectual Rights in Information and Telecommunication Networks'. See KVG Research. December 2013. *TV Market and Video on Demand in the Russian Federation*. Strasbourg, European Audiovisual Observatory, pp. 19–22. www.obs.coe.int/documents/205595/552774/RU+TV+and+VoD+2013+KVG+Research+EN.pdf/5fbb076c-868e-423a-bfed-dca8b66cac43

205 KVG Research, op. cit.

206 Igor Korolev. 17 December 2013. Госдума разрешила блокировать сайты молниеносно и без суда. [Russian Duma decides to block web sites without court permission]. CNews. (In Russian.) www.cnews.ru/news/top/index.shtml?2013/12/17/553820 (Accessed 17 July 2014); No. 292521-6: Bill Passed Protection of Intellectual Property Rights in the Information and Telecommunications Networks. www.copyright.ru/ru/library/zakonoproekti/pravovoe_regulirovanie_in/zakon_292521-6 (Accessed 17 July 2014.)

207 VimpelCom (Beeline). 8 August 2012. Как и почему происходит блокировка сайтов. [How and why websites are blocked/published on the habrahabr website] (in Russian). Beeline telecom blog. http://habrahabr.ru/company/beeline/blog/149249 (Accessed 18 July 2014.)

must comply with government demands, even if they are not accompanied by an official court order, if the content relates to extremism, child pornography, drugs, violence, or the promotion of riots or anti-government actions.[208]

United Kingdom: In the UK, there is no formal definition of an internet intermediary, but 'information society service provider' is defined and would include ISPs and telecommunication companies amongst others, though not as clearly social networks and search engines.[209] Consequently, there is no law in the UK specifically addressing the liability of internet intermediaries per se, but there are a number of laws that de facto address the same. For example, internet services are exempted from liability for defamation if they pass on to a claimant the identity of someone who has posted defamatory material on their site,[210] and under certain situations they may benefit from exclusions of liability for breaches of copyright too.[211] The EU's E-Commerce Directive is a significant source of immunity in general,[212] and the Information Society Directive is a source of relief in copyright claims.[213] Similarly, blocking powers exist, notably for breaches of copyright.[214] In general, courts can compel restrictions on access to material that is a breach of contempt of court laws, or defames, or breaches privacy. In relation to mobile telephony, there are other provisions of particular importance. These derive from the laws relating to Ofcom, the body that grants mobile telephony licenses to all mobile phone network providers. Ofcom has the power to revoke service provider's licenses to protect national security, public safety and health. Ofcom has a duty to act in such a way when directed to by the government. The power and duty is contained in the Communications Act 2003 s 5, and the power to compel Ofcom to act suspend or restrict a particular network provider is contained in section 132. Other powers also exist that

---

208 Roskomnadzor, Government of Russia. 31 January 2014. О вступлении в силу изменений в федеральный закон 'Об информации, информационных технологиях и о защите информации'. [Entry into force of amendments of the Federal Law 'On Information, Information Technologies, and Protection of Information']. (In Russian). Roskomnadzor website. http://rkn.gov.ru/news/rsoc/news23647.htm (Accessed 18 July 2014.)

209 According to Regulation 2 of the ECD Regulations 2002 2013/2002, 'Any service which is normally provided for remuneration, and which operates at a distance by electronic [means], … and at the individual request of a recipient of a service' (relying on recital 17 of Directive 2000/31/EC, commonly known as the E-Commerce Directive). 'It would cover, therefore, most commercial Internet Service Providers, but would not cover internet cafes, whose services are not provided at a distance.'
Lionel Bently and Brad Sherman. 2009. *Intellectual Property Law*, 3rd edn. Oxford, Oxford University Press, p. 158.

210 UK Government. 2013. The Defamation (Operators of Websites) Regulations 2013. The National Archives. www.legislation.gov.uk/ukdsi/2013/9780111104620 (Accessed 18 July 2014.)

211 A source of liability in copyright for ISPs is section 16 of the Copyright Designs and Patents Act 1988, which provides that liability can be imposed where a person: 'without the licence of the copyright owner does, or authorises another to do, any of the acts restricted by the copyright'. UK Government. Copyright, Designs and Patents Act 1988 – Section 16: The acts restricted by copyright. The National Archives. www.legislation.gov.uk/ukpga/1988/48/part/I/chapter/II/crossheading/the-acts-restricted-by-copyright

212 See footnote 154. Under these provisions, liability for damages or criminal sanction is provided for hosting, mere conduit and caching under certain circumstances.

213 Directive 2001/29/EC, Art 5, recently considered by the Supreme Court in *Public Relations Consultants Association Limited v Newspaper Licensing Agency* [2013] UKSC 18. www.bailii.org/uk/cases/UKSC/2013/18.html

214 Article 8(3) of the Copyright Directive, and s97A of the Copyright Design and Patents Act 1988. These are enforced to block websites on the basis of (inter alia) copyright breach. A recent case is *Paramount v BSkyB* [2013] EWHC 3479 (Ch), which also reviews the law on liability for hyperlinks. See www.bailii.org/ew/cases/EWHC/Ch/2013/3479.html

could be used to infringe freedom of expression over mobile communications networks, including a power the government has to issue directions of a general nature to Ofcom or network providers.[215] Prior parliamentary oversight is not required for these powers to be exercised.

United States: Broadly speaking there are two models of internet intermediary liability in the United States. First, Section 230 of the Communications Decency Act (CDA) provides 'expansive protections against liability' from a wide array of speech-based torts, such as defamation, invasion of privacy, misrepresentation and negligence.[216] Section 230 means that search engines are not liable for indexing or linking to potentially illegal third-party content.[217] Section 230 also contains a provision that protects intermediaries such as social networks from liability when they voluntarily block or remove content they determine could be harmful or objectionable to their users. Since the CDA's enactment in 1996, lawsuits attempting to impose intermediary liability have generally buckled under legal scrutiny.[218] Note that the CDA does not shield internet companies against intellectual property claims nor federal criminal laws.

For intellectual property–related claims, Section 512 of the Digital Millennium Copyright Act (DMCA) provides 'conditional safe harbor from liability'.[219] It defines four types of intermediaries – (a) 'transitory digital network communications' (i.e. ISPs), (b) Caching service providers, (c) content hosts and (d) 'information location tools' (i.e. search engines).[220] The DMCA's liability model is characterized as a conditional safe harbour because intermediaries must not have 'actual knowledge' of infringement, not directly benefit from the infringement, and have a notice-and-takedown policy (wherein infringing links are quickly removed from its index, as well as having a termination policy for repeat infringers) in order to gain legal immunity.[221] This conditional model has expanded throughout the world via trade agreements the United States has signed with other countries. It has also served as a template for other countries, including China, India, and the European Union.[222]

---

215 Vodafone, op. cit.; UK Government. Telecommunications Act 1984, s 94 – National Emergency Plans for the Telecommunications Sector. www.gov.uk/government/uploads/system/uploads/attachment_data/file/62282/nep-telecomms-sector-march2010.pdf

216 Adi Kamdar. 6 December 2012. EFF's Guide to CDA 230: The Most Important Law Protecting Online Speech. Electronic Frontier Foundation Deeplinks Blog. https://www.eff.org/deeplinks/2012/12/effs-guide-cda-230-most-important-law-protecting-online-speech (Accessed 2 May 2014.)

217 Eric Goldman. 27 August 2013. When Should Search Engines Ignore Court Orders To Remove Search Results? Forbes. www.forbes.com/sites/ericgoldman/2013/08/27/when-should-search-engines-ignore-court-orders-to-remove-search-results (Accessed 12 April 2014.)

218 Electronic Frontier Foundation. CDA 230 Successes. https://www.eff.org/issues/cda230/successes (Accessed 1 May 2014.)

219 Center for Democracy and Technology, op. cit., pp. 6–13.

220 Legal Information Institute. 17 U.S. Code § 512 – Limitations on liability relating to material online Cornell University Law School. www.law.cornell.edu/uscode/text/17/512 (Accessed 27 March 2014.)

221 Legal Information Institute. 17 U.S. Code § 512 – Limitations on liability relating to material online Cornell University Law School. www.law.cornell.edu/uscode/text/17/512 (Accessed 27 March 2014.)

222 Daniel Seng and Ignacio Garrote Fernandez-Diez. 2012. *Comparative Analysis of National Approaches of the Liability of the Internet Intermediaries*. Geneva, World Intellectual Property Organization, p. 6. www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf

European Union: Intermediary liability in the European Union is largely based on two directives – the E-Commerce Directive[223] and certain provisions of the Information Society (InfoSoc) Directive are particular to claims for breach of copyright.[224] The E-Commerce Directive provides a safe harbour, in general terms, for 'information society services' against 'liability', but not injunctions, for material they carry in certain circumstances.[225] An 'information society service' is defined as: 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service'.[226] The conditions are, in essence, when the information society service is a mere conduit for information, caches it or is a host for it.[227] The Information Society Directive applies only to claims in copyright. It provides that where there is a temporary act of reproduction, there is no breach of a copyright holder's reproduction right – and hence provides a safe harbour against liability. 'Temporary' is further defined as: 'transient or incidental, and an integral and essential part of a technological process and whose sole purpose is to enable (a) a transmission in a network between third parties and an intermediary, or (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance'.[228]

Both Directives have been challenged in court due to what critics consider ambiguity of the defences and safe harbours. For example, the application of the Information Society Directive defence contained in Article 5 has been the subject of eight years of litigation, with a Danish case being referred twice to the Court of Justice of the European Union (CJEU),[229] and a UK case reaching the Supreme Court of the United Kingdom and also being referred to the CJEU.230 The question in this latter case – the 'Meltwater' litigation – included the rather basic issue of whether browsing breached copyright; and the Danish litigation – the 'Infopaq' cases – included the equally fundamental question of the extent to which additional profit made by a defendant vitiates an Article 5 defense.

---

223 European Parliament and the Council of the European Union. 8 June 2000. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). EUR-Lex. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML

224 European Parliament and the Council of the European Union. 22 May 2001. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. EUR-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001L0029

225 Directive 2000/31/EC, op. cit., Articles 12, 13 and 14, Recital 45.

226 Directive 2000/31/EC, Recital 17, Articles 2 (a) and (b), and Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC

227 Directive 2000/31/EC, op. cit., Articles 12, 13 and 14.

228 Directive 2000/31/EC, op. cit., Article 5.

229 *Infopaq International A/S v Danske Dagblades Forening*, ('Infopaq I') Case C-5/08; *Infopaq International A/S v Danske Dagblades Forening*, ('Infopaq II') Case C-302/10. Maria Fredenslund. 17 May 2013. Denmark: Infopaq-case finally decided after eight years. Kluwer Copyright Blog. http://kluwercopyrightblog.com/2013/05/17/denmark-infopaq-case-finally-decided-after-eight-years (Accessed 17 July 2014.)

230 *Public Relations Consultants Association Ltd v Newspaper Licensing Agency* [2013] UKSC 18. www.bailii.org/uk/cases/UKSC/2013/18.html (Accessed 18 July 2014); *Newspaper Licensing Agency Ltd and others v Public Relations Consultants Association Ltd* (Case C-360/13)

Ambiguities also exist in the E-Commerce Directive.[231] So, for example, the protection of the Directive for hosts is lost when a defendant has 'actual knowledge' of illegal activity or of facts from which illegality becomes apparent, but it is not clear what constitutes 'actual knowledge'.[232] Indeed, the regulation does not specify what information is required in a notice that purports to provide a defendant with such knowledge, and hence remove the defense. This, conceivably, may be different when a defendant is being sued in copyright or defamation. Further, and also in relation to liability for hosts and caching, the law says that a defendant needs to act 'expeditiously to remove or disable access to the information', but does not indicate how long 'expeditiously' should be.[233] These ambiguities can create a chilling effect on expression, and an interference with freedom of expression, as companies will be automatically tempted to take down content about which they have been served a notice. This is because evaluating the merits of the case will take time and money, and it may be more efficient, cheaper and without the risk of liability, as noted earlier in the explanation on the safe harbour model, to react and remove, rather than pause and think.[234]

2.2.3 Special Note: Intermediary Liability in Sub-Saharan Africa

While internet usage is growing fastest in the developing world, legal provisions related to intermediary liability have yet to catch up in many parts of Sub-Saharan Africa.[235] Absence of intermediary liability provisions creates regulatory and procedural uncertainty.[236] A 2014 report by an international NGO with consultative status to the UN's Economic and Social Council, the Association for Progressive Communications (APC), argues that the lack of protection for intermediaries in African countries causes intermediaries to proactively restrict content on their networks and platforms, resulting in the undue restriction of users' freedom of expression.[237]

Many African countries are in the process of crafting intermediary liability regimes, partly in response to approaches by international bodies and major trade and aid partners to protect intellectual property rights and ensure that intermediaries take action against copyright-infringing material on their networks and platforms.[238]

Some countries, such as **South Africa** and **Uganda**, have adopted safe harbours modeled on those of the United States and the European Union, although they have

231 Ashley Hurst, Partner at Olswang LLP. Interview with Richard Danbury. Personal interview. Cambridge/London, UK, 14 April 2014. This paragraph gratefully draws on Mr Hurst's critique, but errors remain our own.
232 Art 14 (a)
233 Art 13 (e), Art 14 (b), recital 46
234 Ashley Hurst. 25 January 2013. ISPs and defamation law: hold fire, Robert Jay. *The Guardian*. www.theguardian.com/law/2013/jan/25/defamation-law-robert-jay (Accessed 17 July 2014.)
235 For example, it has been found that South Africa and Uganda have legal provisions explicitly addressing intermediary liability, but in countries such as Kenya and Nigeria, intermediary liability is an emerging debate and issue. Comninos, An Uncertain Terrain, op. cit., p. 4.
236 Ibid. p. 12.
237 Gandhi, op. cit.
238 Ibid.

been implemented quite recently and thus so far there is little 'clarifying jurisprudence'.[239] In **South Africa**, Chapter XI of the Electronic Communications and Transactions Act 'provides for the limitation of liability for service providers, if these providers are members of an industry representative body that has been recognized by the minister, and they have adopted that body's code of conduct' (emphasis added).[240]

Regulatory uncertainty can stem from new laws that muddy the intent of previous laws. For example, **Uganda**'s Electronic Transactions Act of 2011 limits the liability of service providers for user content and, furthermore, it does 'not require them to monitor stored or transmitted data including for unlawful activity'.[241] However, since then, ISPs have been compelled to 'install electronic surveillance and interception equipment that "identifies the origin, destination, termination, duration and equipment identification of each communication"'.[242]

On the other hand, Kenya and Nigeria – countries with high internet penetration rates and vibrant tech communities – lack intermediary liability regimes.[243] **Nigeria** has proposed provisions addressing liability of telecommunication providers for subscribers' activity. Such provisions are coupled with provisions addressing data retention.[244] In **Kenya**, companies have begun to create policies restricting user activity and content in an effort to pre-empt legal action over defamatory content.[245]

For countries putting in place intermediary liability regimes, civil society groups concerned with freedom of expression such as Association for Progressive Communications have voiced concern that countries will 'cherry pick' from other countries' regimes.[246] This can

---

239 Alex Comninos. October 2012. *Intermediary liability in South Africa*. South Africa, Association for Progressive Communications, p. 9. (Intermediary Liability in Africa Research Papers, No. 3). www.apc.org/en/system/files/Intermediary_Liability_in_South_Africa-Comninos_06.12.12.pdf

240 Republic of South Africa. 31 July 2002. Electronic Communications and Transactions Act, 2002 (No. 25 of 2002.) www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislations/South%20Africa/ElecComm.PDF (Accessed 31 July 2014.); Guy Berger and Zikhona Masala. 22 March 2012. *Mapping Digital Media: South Africa*. New York, Open Society Foundations, p. 98. www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-south-africa-20120416.pdf

241 Ashnah Kalemera. 20 June 2014. *Uganda: When National Security Trumps Citizens' Internet Freedoms*. OpenNet Africa. http://opennetafrica.org/internet-freedom-in-uganda-personal-information-and-the-state (Accessed 11 July 2014.)

242 Ashnah Kalemera, Lillian Nalwoga and Wairagala Wakabi. Intermediary Liability in Uganda. CIPESA. (Intermediary Liability in Africa Research Papers, No. 5.) www.apc.org/en/system/files/Intermediary_Liability_in_Uganda.pdf (Accessed 29 July 2014.)

243 Kenya and Nigeria have a 36.70 per cent and 37.5 per cent penetration rate, respectively, where an internet user is defined as an 'individual, of any age, who can access the Internet at home, via any device type (computer or mobile) and connection'. Internet users in both countries have grown at the high annual rate 16 per cent. Interestingly, because Nigeria has such a large population (at 178 million people, it has the eighth-largest population of internet users worldwide – behind Germany and ahead of the UK. See Internet Users by Country. 2014. Internet Live Stats. www.internetlivestats.com/internet-users-by-country (Accessed 15 July 2014.)

244 Gbenga Sesan. 16 May 2014. New Laws Affecting Intermediary Liability in Nigeria. *APCNews*. www.apc.org/en/node/19200 (Accessed 17 July 2014.)

245 Grace Githaiga. 19 May 2014. Intermediary Liability: Preventing hate speech online in Kenya. *APCNews*. www.apc.org/en/node/19202 (Accessed 17 July 2014.)

246 Ibid.

lead to unintended consequences, they fear, because the importation of provisions is not always complete, and can translate into more stringent, broad or vague regulations.[247]

Another concern is that countries may establish restrictive and selective regimes. Because monitoring by intermediaries for potential illegal content could compromise internet users' right to privacy and freedom of expression, strong data protection and privacy laws have been identified as an important safeguard to ensure that intermediary liability regimes are not abused for surveillance or monitoring purposes.[248] Indeed, while the lack of intermediary liability regimes weakens freedom of expression, the simple existence of an intermediary liability regime does not guarantee stronger protection either for intermediaries or for online freedom of expression in general. In addition, intermediaries' own terms of service may be inadequately aligned to freedom of expression standards. Competence of the courts and the presence of entities able to advocate for online human rights are key to ensuring protection of intermediaries and online freedom of expression.[249]

2.3 Self-regulation and Co-Regulation

Laws are not the only source of online content restriction; a company's private rules like its 'terms of service' also circumscribe freedom of expression. For example, Facebook[250] and YouTube[251] do not allow pornography, but Google's Blogger does – as long as that content is not accompanied by advertisements.[252] Blogger also does not allow gratuitously bloody content such as 'close-up images of gunshot wounds or accident scenes without additional context or commentary'.[253] Pornography and photos of gunshot wounds are not illegal in the United States, where Facebook and Google are headquartered, but the companies has made the decision to exclude such content on the rationale this would as they 'serve to enhance the service as a whole'.[254]

Additionally, while US law protects hate speech as long as it would not incite imminent violence, most US-based companies proscribe much broader categories of hate speech in their terms of service.[255]

---

247 Nicolo Zingales. November 2013. *Internet intermediary liability: Identifying best practices for Africa*. South Africa, Association for Progressive Communications, p. 25. www.apc.org/en/system/files/APCInternetIntermediaryLiability_BestPracticesAfrica_20131125.pdf

248 Githaiga, op. cit.

249 Comninos and Rens, op. cit.

250 Facebook Community Standards. https://www.facebook.com/communitystandards

251 YouTube. YouTube Community Guidelines. https://www.youtube.com/t/community_guidelines

252 Violet Blue. 28 June 2013. Google's Blogger to delete all 'adult' blogs with ads in three days. ZDNet. www.zdnet.com/googles-blogger-to-delete-all-adult-blogs-with-ads-in-three-days-7000017451 (Accessed 31 July 2014.)

253 Google. Blogger Content Policy. www.blogger.com/content.g?hl=en

254 Ibid.

255 For example, Blogger: 'content that promotes or condones violence against individuals or groups based on race or ethnic origin, religion, disability, gender, age, nationality, veteran status, or sexual orientation/gender identity, or whose primary purpose is inciting hatred on the basis of these core characteristics'; Facebook: 'Content that attacks people based on their actual or perceived race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability or disease is not allowed. We do, however, allow clear attempts at humor or satire'; YouTube: 'speech which attacks or demeans a group based on race or ethnic origin, religion, disability, gender, age, veteran status, and sexual orientation/gender identity'.

In some jurisdictions, systems to set and enforce rules for online expression combine elements of public and private authority, resulting in self-regulation and co-regulatory enforcement mechanisms. The scope and power of these mechanisms are in turn heavily shaped by states' legal and regulatory contexts. Thus there is a great deal of fluidity and inter-linkage between public and private regulation. All of the internet intermediaries covered in this report engage in some degree of self-regulation and private enforcement. The extent and nature of self- regulation and co-regulation taking place in a given jurisdiction is in turn shaped by the specific constitutional, legal and regulatory frameworks of that jurisdiction, particularly its intermediary liability regime.

The four international rapporteurs on freedom of expression – UN Special Rapporteur on Freedom of Opinion and Expression; OSCE Representative on Freedom of the Media; Organization of American States (OAS) Special Rapporteur on Freedom of Expression; and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information – have pronounced self-regulation to be an 'effective tool in redressing harmful speech' which 'should be promoted'.[256] In fact, as early as 2003 self- and co-regulation was viewed favourably; a Council of Europe declaration encouraged 'self-regulation or co-regulation regarding content disseminated on the Internet' by member states.[257] If such systems are not to serve as censorship, they should operate in terms of criteria and processes aligned to international stand ards on freedom of expression.

Company self-regulation: At the level of the individual company this ranges from measures taken by the company to block or remove spam and viruses, to the setting and enforcement of 'terms of service', which are rules that users must agree to abide by in order to use the service. The case studies demonstrate that the terms of service for one company may be very similar to legal and regulatory requirements, whereas other companies prohibit content that is legal but deemed by the company to be undesirable or incompatible with the purpose or character of its service.

Private companies are legally allowed to draft their own terms for what constitutes undesirable content (for example, companies targeting children may prohibit cursing). However, because large internet intermediaries effectively serve as quasi-public spheres, some advocates have argued that these companies have a responsibility to assess the human rights implications of their private rules in order to minimize negative impact on users' rights.[258]

Collective self-regulation: A group of private entities may jointly create industry codes of conduct or set common technical standards by which all participants agree to abide.

---

256 Adeline Hulin (ed). 2013. *Joint Declarations of the representatives of intergovernmental bodies to protect free media and expression*. Vienna, Organization for Security and Co-operation in Europe, p. 67. www.osce.org/fom/99558?download=true

257 Council of Europe Committee of Ministers. 28 May 2003. Declaration on freedom of communication on the Internet. (Decl-28.05.2003E.) https://wcd.coe.int/ViewDoc.jsp?id=37031 (Accessed 30 October 2014.)

258 Jillian C. York. September 2010. Policing Content in the Quasi Public Sphere. OpenNet Initiative. https://opennet.net/policing-content-quasi-public-sphere (Accessed 17 July 2014.)

As internet scholar Christopher Marsden defines it: 'a group of firms or individuals exert control over their own membership and behavior. Membership is voluntary and participants draw up their own rules using tools such as codes of conduct as well as technological solutions and standards. Members take full responsibility for monitoring and compliance without reference to a statutory regulatory authority'.[259]

One example of such an arrangement is the 'six strikes' Copyright Alert System adopted by major US internet service providers, in which the companies have agreed to adhere to common practices to monitor their networks for copyright infringement and to target and alert users alleged to have infringed.[260] Executed by the non-profit Center for Copyright Information[261] the scheme allows service providers to adapt its basic underlying principles as they see fit. As a result, the implementation of the scheme reportedly varies from service provider to service provider: some warn users and reduce their internet speeds, while others block access to specific websites until the user takes courses in copyright and piracy awareness.[262]

Co-regulation: A growing amount of self-regulation, particularly in the European Union, is implemented as an alternative to traditional regulatory action. Some governments actively encourage or even place pressure on private business to self-regulate as an alternative to formal legislation or regulation which is inherently less flexible and usually more blunt than private arrangements.[263] A regulatory regime involving private regulation that is actively encouraged or even supported by the state through legislation, funding, or other means of state support or institutional participation, has come to be known as 'co-regulation'.[264]

A global example of co-regulation is a notice-and-takedown system to combat child sexual abuse images established between the International Association of Internet Hotlines (INHOPE) and ISPs.[265] Of the countries addressed in this report, Brazil, Germany, Hungary, Russia, the UK and the United States operate INHOPE-associated hotlines.[266]

Specifically in the **UK**, the Internet Watch Foundation (IWF), a self-regulatory body set up by the internet industry in 1996 in response to the threat of more direct regulation, is empowered to make decisions about what content should be blacklisted, while working

---

259 Christopher T. Marsden. 2011. *Internet Co-Regulation: European Law, Regulatory Governance, and Legitimacy in Cyberspace*. Cambridge, Cambridge University Press, p. 54.

260 Mitch Stoltz. To Safeguard the Public Domain (and the Public Interest), Fix Copyright's Crazy Penalties. EFF Deeplinks blog. 18 January 2014. https://www.eff.org/deeplinks/2014/01/safeguard-public-domain-and-public-interest-fix-copyrights-crazy-penalties (Accessed April 15, 2014.)

261 Copyright System FAQs. Center for Copyright Information. http://www.copyrightinformation.org/resources-faq/copyright-alert-system-faqs/ (Accessed 15 April 2014.)

262 Matthew Ingram. Should You Fear the 'Six Strikes' Anti-Piracy Rule? 27 February 2013. http://www.businessweek.com/articles/2013-02-27/should-you-fear-the-six-strikes-anti-piracy-rule (Accessed 15 April 2014.)

263 Marsden, op. cit., p. 48.

264 Marsden, op. cit., p. 46.

265 In Germany three such hotlines are operated by the self-regulatory Association for the Voluntary Self-Monitoring of Multimedia Service Providers (FSM e.V.), the Association of the German Internet Industry eco e.V. and the joint state-regulatory body *Jugendschutz*. INHOPE Member Details. https://old.inhope.org/en/hotlines/facts.html (Accessed 18 July 2014.)

266 Ibid.

closely with government departments. In 2014 the IWF was tasked by the UK Government to actively investigate child sex abuse images on the internet.[267] In **Germany**, in addition to complying with warrants and court orders, service providers have developed Codes of Conduct in conjunction with a non-governmental self-regulatory body, the Voluntary Self-Monitoring of Multimedia Service Providers (FSM). These codes include commitments to ensure that content on their networks complies with statutory requirements regarding the protection of youth, including child sexual abuse images.[268] In **Brazil**, the nongovernmental organization Safernet accepts anonymous complaints of human rights violations on the internet relating to child sexual abuse images (online paedophilia), in addition to racism, xenophobia, religious intolerance, neo-Nazism, incitement to crimes against life, homophobia, and incitement to cruel treatment of animals.[269] Safernet investigates the complaint, and collaborates with the federal police and prosecutors' office, which may start a criminal investigation. If there is enough evidence that a site has hosted content that was found to be illegal, the site will be asked to remove the illegal content and is required to preserve evidence of the alleged crime. The content of the users' communications may only be shared if there is a court order, however, demonstrating possible privacy implications of such cooperations.[270]

Proponents of the co-regulatory model are seeking to expand it. For example in 2013 the UK government established an *Extremism Taskforce*, which among other things, committed to working with service providers to restrict access to online extremist material hosted overseas, but illegal in the UK. The task force also sought to strengthen mechanisms for public reporting of online extremist content, and work with the internet industry – in a co-regulatory capacity to identify and include extremist content in 'family friendly' filters.[271] According to media reports in 2013, the government was considering establishing a system similar to the Internet Watch Foundation, in which a government funded body would identify and work with service providers to block or otherwise disable extremist content.[272]

All three of the case studies in this report examine various models of self- and co-regulation. Proponents of industry self-regulation argue that it is preferable to government regulation because such coordination is more flexible and more effective than government regulation, deters legal yet undesirable conduct in the context of a particular service's

---

267 Internet Watch Foundation. 2013. Internet Watch Foundation Annual & Charity Report 2013. Cambridge, IWF, p. 5. www.iwf.org.uk/assets/media/annual-reports/annual_report_2013.pdf.pdf (Accessed 29 July 2014.)

268 Jugendmedienschutz im Mobilfunk.Selbstverpflichtung der Mobilfunkanbieter [Youth Protection in Mobile Networks. Code of Conduct of Mobile Providers],. October 2007. http://www.izmf.de/sites/default/files/download/Studien/jugendschutz_mobilfunk.pdf (Accessed 12 April 2014.)

269 O Que Denunciar. Safernet Brasil. http://www.safernet.org.br/site/institucional/projetos/cnd/o-que-denunciar.

270 Term of Cooperation, article 5, paragraph 1. Available at: http://www.safernet.org.br/site/sites/default/files/Teles.pdf

271 Tackling extremism in the UK: Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism. HM Government. December 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/263181/ETF_FINAL.pdf

272 Juliette Garside. Ministers will order ISPs to block terrorist and extremist websites. The Guardian. 17 November 2013. http://www.theguardian.com/uk-news/2013/nov/27/ministers-order-isps-block-terrorist-websites (Accessed 7 July 2014.)

purpose, helps consumers evaluate products and services, and can lead to more efficient product standards in addition to lowering the cost of production. On the other hand, critics warn that self-regulation's frequent shortfalls in regard to public accountability and due process may fail to protect democratic values and neglect basic standards of justice.[273] For example, the European Digital Rights Initiative warned that 'very basic questions need to be asked about whether we should entrust enforcement of law in a core element of modern democracy – electronic communications – to private companies'.[274] The European Commission has argued that co-regulation is ill-suited for situations in which 'fundamental rights or major political choices' are at stake.[275]

2.4 Introducing the Case Studies

With the legal and regulatory context clearly established, the next three chapters examine ISPs, search engines and social networks in turn – examining the extent to which individuals' rights are respected when their freedom of expression depends on private sector internet intermediaries.

The three case studies illustrate how an internet user's freedom of expression hinges on the interplay between a company's policies and practices, government policy, and geopolitics. Key questions include: To what extent do companies make concerted efforts to respect users' rights in the face of government requests and legal frameworks that are not always consistent with international human rights norms? What is the impact of private terms of service on freedom of expression?[276] In addition to limitations on content, to what extent do company data protection practices and privacy policies, combined with government surveillance requirements, affect whether people can freely express themselves?[277]

Clearer understanding of such outcomes by all stakeholders should in turn help foster freedom of expression online: helping governments formulate laws that protect online rights but also facilitate intermediaries' respect for users' rights; helping companies improve their policies and practices to foster freedom of expression via their services; and helping civil society hold governments as well as companies accountable.

---

273 Konstantinos Komaitis. 29 July 2013. Voluntary Initiatives as a source of policy-making on the Internet. Internet Society Public Policy blog. www.internetsociety.org/blog/2013/07/voluntary-initiatives-source-policy-making-internet (Accessed 28 July 2014.)

274 Joe McNamee. January 2011. *The Slide from Self-Regulation to Corporate Censorship*. Brussels, European Digital Rights Initiative, p. 5. www.edri.org/files/EDRI_selfreg_final_20110124.pdf

275 European Commission. 12 October 2001. European Governance: A White Paper. *Official Journal of the European Communities*. (2001/C 287/01.) p. 17. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0428&rid=2

276 Article 19, 'Dilemma', op. cit., p. 7.

277 La Rue, A/HRC/23/40, op. cit., pp. 19–20.

3. STUDY 1: INTERNET SERVICE PROVIDERS

Vodafone (UK, Germany, Egypt), **Vivo/Telefônica Brasil** (Brazil), **Bharti Airtel** (India, Kenya), **Safaricom (Kenya)**

3.1 Introduction

Internet service providers (ISPs) allow users to access and use the Internet via fixed line or wireless connections.[278] They enable the transmission of data to and from other intermediaries (such as search engines, social networking platforms, web hosting services, cloud computing services, etc.) over their networks.

ISPs can be state-owned, partially privatized or fully privatized.[279] Many are operated by companies whose original business focused on traditional and mobile telephone services prior to expanding into internet services. Companies that act as ISPs may also provide other services like voice calling, web hosting, cloud computing, domain name registration, email, and other services. This case study focuses on the core functions of an ISP as a provider of internet access via wireless and fixed-line services.

As the Guiding Principles of the Telecommunications Industry Dialogue on Freedom of Expression and Privacy point out, telecommunications can both enhance openness and transparency, and are pertinent to governments in protecting public safety and security.[280] ISPs play a critical role in facilitating the right to freedom of expression given that internet access is not only a prerequisite for online expression, but for enabling the free flow of information globally.[281] They act as internet 'gatekeepers'[282] given their direct access to, and the technical ability to restrict, voice or data communication on their networks.

---

278 The Economic and Social Role of Internet Intermediries. OECD. DSTI/ICCP(2009)9/FINAL, p.9. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2009)9/FINAL&doclanguage=en

279 Tuppen, op. cit. p. 10.

280 Telecommunications Industry Dialogue on Freedom of Expression and Privacy. Guiding Principles. Version 1 6 March 2013. http://www.vodafone.com/content/dam/sustainability/pdfs/telecom_industry_dialogue_principles.pdf

281 Comments of The New America Foundation, Free Press, Electronic Frontier Foundation, Public Knowledge, Reporter Without Borders, American Civil Liberties Union. Before the National Telecommunications and Information Administration, U.S. Department of Commerce. In the Matter of Global Free Flow of Information on the Internet. Docket No. 100921457–0457–01. 6 December 2010. p.3. http://www.ntia.doc.gov/files/ntia/comments/100921457-0457-01/attachments/NAFetal_FreeFlowofInfoComments.pdf

282 Shielding the Messengers: Protecting Platforms for Expression and Innovation. Version 2. Center for Democracy and Technology. December 2012. p.20. https://www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf

ISPs also have the ability to collect, store, and gain access to user's personal data and the content of their communications as well as metadata such as IP addresses, call record details, and location.[283] They can face legal mandates, and even extra-legal interference through informal pressures, to provide access to this information, and can also face legal requirements to facilitate real time monitoring and surveillance.[284] For these reasons ISPs' roles at the network level can affect users' freedom of expression on other intermediaries' services such as search engines and social networking platforms.

The business models of ISPs – provision of internet access to fixed line or mobile subscribers – generally requires the investment of substantial physical infrastructure, equipment, and personnel in the jurisdictions where they themselves or the telecommunications providers operate.[285] Thus, their policies and practices affecting freedom of expression map more closely to a jurisdiction's political and legal context than that of other intermediary types such as search engines or social networking platforms outside of their home jurisdiction. Nonetheless, this case study demonstrates that ISPs do have control over a range of company business decisions, policies and practices that affect freedom of expression online.

Publicly available terms of service, Privacy Policies, and other relevant policy documents of the companies were analysed in the context of news items, stakeholder interviews, and applicable legislation of the relevant jurisdictions in order to understand the challenges ISPs face in respecting the right to freedom of expression.

3.1.1 The Companies

This case study examines the following ISPs operating in Brazil, India, the United Kingdom, Germany, Egypt, and Kenya:

Vivo Telecommunications:[286] Vivo Telecommunications, also known as Telefônica Brasil, was launched in 1993. With 79 million cell phone subscribers as of May 2014, Vivo is the largest telecommunications company in Brazil,[287] and offers mobile, broadband, and cable services.[288] For the purposes of this research, Vivo operations were studied in Brazil, with particular attention to the terms of service for internet services of mobile 'post pay' monthly subscribers.[289]

283 Dunstan Alliston Hope. Protecting Human Rights in the Digital Age. BSR. February 2011. https://globalnetworkinitiative.org/sites/default/files/files/BSR_ICT_Human_Rights_Report.pdf
284 Ibid.
285 Telecommunication Industry Dialogue. Guiding Principles. op. cit.
286 Vivo's website. http://www.vivo.com.br/portalweb/appmanager/env/web.
287 Market Share das Operadoras de Celular no Brasil. Teleco. 17 June 2013. http://www.teleco.com.br/mshare.asp (Accessed 24 June 2014.)
288 www.vivo.com.br
289 CONTRATO DE ADESÃO AO SERVIÇO VIVO INTERNET MÓVEL PÓS PAGO (Contract for membership to the service Vivo Mobile Internet Postpaid). http://www.vivo.com.br/consumo/groups/public/documents/documentopw/ucm_009621.pdf

Bharti Airtel:[290] Bharti Airtel is an Indian multinational telecommunications business founded in 1995. Airtel offers 2G, 3G and 4G wireless services, mobile commerce, fixed-line services, high speed DSL broadband, IPTV, DTH, enterprise services including national and international long-distance services to carriers in twenty countries. Airtel is ranked as the world's fourth largest mobile operator with a subscriber base of over 200 million.[291] For the purposes of this research, Airtel operations were studied in India and Kenya.[292] Airtel India's 'Terms and Conditions for Providing Services'[293] and the 'Online Privacy Policy'[294] and Airtel Kenya's 'Terms and Conditions for the Use of Airtel Data'[295] were reviewed.

Vodafone:[296] Vodafone is a UK-based multinational telecommunications business founded in 1991. Vodafone is the world's second-largest telecommunication provider with a subscriber base of over 411 million customers and operating businesses in 29 countries in addition to joint ventures like Kenya's Safaricom, which Vodafone calls its 'local associate operator' (see below).[297] For the purposes of this research, Vodafone was studied in the UK, Germany and Egypt. For Vodafone UK and Vodafone Germany, the 'Terms and Conditions: General Terms' were reviewed. Additional policy documents from the Vodafone Group such as the 2014 'Disclosure to Law Enforcement Report' were reviewed.[298]

Safaricom:[299] Safaricom is Kenya's largest mobile operator with 21 million subscribers.[300] According to Bloomberg Industries, Safaricom claims 67 per cent of Kenya's mobile-phone market, as well as 79 per cent of voice traffic and 96 per cent of text messages as of March 2014.[301] Safaricom is 40 per cent owned by Vodafone; the Kenyan Government owns 35 per cent and the remaining shares were publicly floated on the Nairobi Stock

290 www.airtel.in
291 About Bharti Airtel. Airtel India. http://www.airtel.in/about-bharti/about-bharti-airtel Airtel crosses 200 million mobile customer mark in India. 19 February 2014. http://www.airtel.in/about-bharti/media-centre/bharti-airtel-news/corporate/airtel-crosses-200-million-mobile-customer-mark-in-india;
292 For more information about Airtel Kenya, see: http://africa.airtel.com/wps/wcm/connect/africarevamp/Kenya//.
293 Airtel India. Terms and Conditions for Providing Services. https://cloud.airtel.in/ap4saasWeb/terms-conditionsForUserReg.html
294 Online Privacy Policy. Airtel. http://www.airtel.in/forme/privacy-policy
295 Airtel Kenya. Terms & Conditions for the use of Airtel Data. http://africa.airtel.com/wps/wcm/connect/africarevamp/kenya/3g/home/terms-and-conditions
296 www.vodafone.com
297 Factsheet. Vodafone Group Plc. http://www.vodafone.com/content/dam/vodafone/investors/factsheet/group_factsheet.pdf
298 Vodafone UK. Terms and conditions: General terms. http://www.vodafone.co.uk/about-this-site/terms-and-conditions/general-terms/
299 www.safaricom.co.ke
300 For more information see: http://www.safaricom.co.ke/about-us/investors-relations/investor-dashboard/corporate-information.
301 Eric Ombok. 26 March 2014. Vodafone's Safaricom May Withdraw Its Offer for Essar Kenya. *Bloomberg*. www.bloomberg.com/news/2014-03-25/safaricom-may-drop-bid-for-essar-kenya-unit-over-regulator-delay.html (Accessed 14 August 2014.)

Exchange in June 2008.[302] The 'Safaricom Post Pay Customer Terms and Conditions' and 'Conditions of Use for the Safaricom Prepaid Services' were reviewed.[303]

3.2 Direct Restrictions on Freedom of Expression

In this report's introduction (Chapter 1), the section on 'Modes of Restriction' lists three primary ways that internet intermediaries can restrict expression. Restrictions carried out by ISPs are 'network-level' restrictions because they either prevent or restrict an individual's access to the internet itself or prevent or restrict access to online content, expression opportunities, and services that are offered by other types of intermediaries. As case studies 2 and 3 will demonstrate, network-level restrictions made by ISPs affect the nature and extent of restrictions carried out by other intermediaries such as search engines and social networking platforms.

3.2.1 Network-Level Filtering

Filters are specialized software programs that can restrict access to entire websites, types of online services, specific pages or content within websites, or web pages containing specified keywords.[304] State-mandated filtering is usually carried out by ISPs and can be required as one of the conditions of a company's operating license in a jurisdiction. The state may also install centralized filtering mechanisms through internet exchange points that serve as gateways for internet traffic between different jurisdictions and to - and from - the networks operated by different ISPs. Private or local institutions such as schools and libraries can deploy filters on their own local networks to block access to certain content. Filters can also be installed at the household level – most commonly by parents seeking to control what content their children can access.[305] This report focuses primarily on state-mandated filtering by ISPs as well as other filtering that ISPs might deploy to

302 John Maina. 3 October 2007. Scramble for Safaricom: Who is Fooling Who? *The African Executive*. www.africanexecutive.com/modules/magazine/articles.php?article=2590&magazine=143 (Accessed 14 August 2014); Kurt Eilhardt. 2010. Safaricom: Managing Risks in a Frontier Capital Market. The Fletcher School at Tufts University. http://fletcher.tufts.edu/IBGC/Lab/StudentResearch/~/media/Fletcher/Microsites/CEME/newpdfs/SafaricomFinal112010.ashx (Accessed 14 August 2014.)

303 Though both of these Terms and Conditions refer to mobile services, they are the core Terms and Conditions for services such as data bundles powered by 3G. These Terms and Conditions include information about subscription and allocation, but note that they are extensions of the Post Pay and Pre Paid Terms and Conditions. For access to Safaricom post pay Terms and Conditions see: http://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/standard_terms_conditions_safaricom_postpay_service_v1_feb_2010_tracked.pdf. For access to Sarfaricom Pre Pay Terms and Conditions see: http://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/conditions_of_use_for_the_safaricom_prepaid_services.pdf

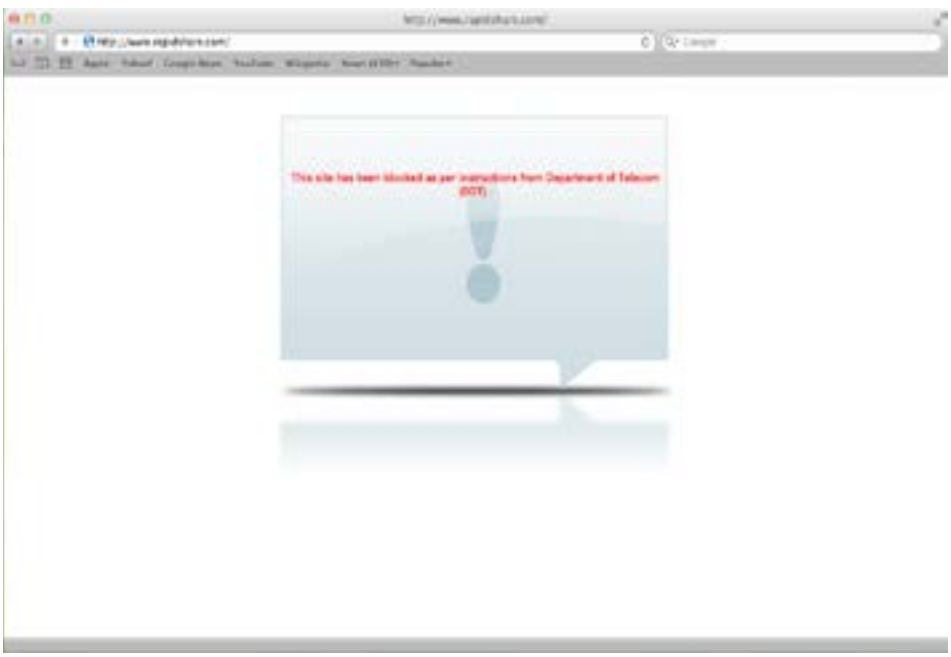
304 R. S. Rosenberg. 2011. Controlling access to the Internet: The role of filtering. *Ethics and Information Technology*, Vol. 3, No. 1, pp. 35–54. www.copacommission.org/papers/rosenberg.pdf

305 Jonathan Zittrain and John Palfrey. Internet Filtering: The Politics and Mechanisms of Control. In Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds. Access Denied: The Practice and Policy of Global Internet Filtering. (Cambridge: MIT Press) 2008. pp 6-8. Online at: http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-2.pdf

enforce their own rules, or to participate in collective industry self- and co-regulation (see Chapter 2 for a discussion of private regulatory mechanisms).

Through deployment of specialized filtering technology, ISPs can filter specific keywords or URLs belonging to specific web pages. With very basic techniques they can also filter entire websites at the network level, as in the example depicted below.

Figure 1: screenshot of browser attempting to visit a filtered file-sharing website in India in 2011.[306]



When content or a URL within a website is filtered at the network level, users can only reach the unfiltered part of the website. When an entire website is filtered at the network level, the user cannot reach any part of that website. Under the latter it is possible that even legal content is also rendered inaccessible.

Depending on the legal context, ISPs can receive requests, recommendations, and orders for filtering from the government, private third parties, and/or regulatory organizations. Such orders can be communicated on a case-by-case basis directly to the ISP, or in the form of a general 'blacklist'. Examples from this research demonstrate that some ISPs in some jurisdictions take self-regulatory or co-regulatory steps - including vetting content on their networks by standards developed by the company, as well as collaborating with hotlines, regulatory, and industry bodies to identify infringing content. ISPs can also offer

306 Online at: http://www.medianama.com/wp-content/uploads/Screen-Shot-2011-07-21-at-10.55.41-AM.png

individual users the option of applying filters to their home and office networks. Freedom of expression can be affected by the reasons for filtering, the practical implementation of the filtering, and the transparency by government and companies about how and why the filtering occurs.

Company Policy

Case study research focused on company policies on complying with government and other parties' requests and how they enforce their private terms of service. Because the researchers were unable to secure interviews with company representatives, the following relies on publicly available sources.

Compliance with government requests: Airtel India blocks websites, content, and specific user accounts as directed by statutory authorities or security agencies.307 The Vodafone Group broadly clarifies in a document titled 'An Overview of Vodafone's policy on privacy, human rights, and law enforcement assistance' that the company will assist law enforcement where legally required.308 Vodafone also explains in its 'Law Enforcement Disclosure Report' that the company may apply filters as mandated by authorized authorities and according to 'block lists' maintained by relevant authorities.309 Airtel Kenya, and Safaricom do not address how they comply with government filtering requests in publicly available materials, although Vodafone included Safaricom, of which it owns a 40 per cent stake, in the 'Law Enforcement Disclosure Report' as 'Vodafone's local associate operator'.[310] It is unclear to what extent Vodafone's policy on privacy, human rights, and law enforcement assistance extends to cover Safaricom in absence of clarification by Safaricom. Vivo does not mention the issue of government filtering requests in its public materials but that has become moot since the Marco Civil da Internet prohibits filtering of content.[311]

Enforcement of private rules: As a co-regulatory step, Vodafone UK clarifies that it collaborates with the Internet Watch Foundation (IWF) to filter content specifically related to child sexual abuse which is identified and communicated by the IWF in the form of a block list.[312] (See Chapter 2 for in-depth discussion of co-regulation generally and the IWF specifically.) Vodafone has a license to use the IWF blacklist in territories outside of

307 Airtel India. Terms and Conditions for Providing Services. Section 15.5.8. op. cit.
308 Vodafone. Human Rights and Law Enforcement. 17 July 2012. http://www.vodafone.com/content/index/about/about-us/privacy/human_rights.html.
309 Vodafone Law Enforcement Disclosure Report. op. cit. p. 68.
310 Ibid. p. 78.
311 Isabel Costa Carvalho, Claudette M. Christian, Timothy P. Tobin and Arthur Rodrigues do Amaral. Marco Civil da Internet: Brazil's new Internet Law could broadly impact online companies' privacy and data handling practices. Lexology: Association of Corporate Counsel. 7 May 2014. http://www.lexology.com/library/detail.aspx?g=2b5808f2-a0a6-469f-ba05-4b2335dfb36f (Accessed 14 August 2014.)
312 Human Rights – Our approach. Vodafone. http://www.vodafone.com/content/sustainability/operating_responsibly/human_rights.html

the UK.[313] As a self-regulatory step, Vodafone UK and Vodafone Germany also provide customers with the option to activate parental controls and filter content.[314]

All companies include in their Terms prohibited types of content and activities on their networks. Specificity varies, but most use broad terms to capture many forms of disallowed content. For example, Airtel India prohibits what it calls objectionable, obscene and pornographic messages or communications, and maintains that content and communications on the network must be consistent with Indian law.[315] Airtel Kenya requires users to comply with all relevant laws and regulations and notes that users cannot encourage, allow or engage in the transmission of what it terms obscene or offensive communications, the spread of viruses, copyright infringing material, or defamatory material.[316] Safaricom's pre-paid terms of service hold users responsible for any transmitted material/communication, which is classified as illegal, defamatory, misleading or in breach of any persons rights.[317] (These conditions do not apply to Safaricom's 'post pay' or monthly subscriber service terms.)

In contrast, Vodafone UK filters access to web or Wireless Application Protocol (WAP) sites that are known or suspected to be illegal, and places mandatory restriction and verification controls on content that is restricted to individuals 18 years and older.[318] Among other prohibited uses, Vodafone Germany obliges the customer to avoid violating third-party rights, in particular copyright and trademark rights.[319] Vivo says that it prohibits acts that are contrary to law, moral, good customs, and customs and habits understood to be reasonable and acceptable online. This includes dissemination of messages that are racist, pornographic, paedophilic, intellectual property–infringing, or that violate the law.[320] Vivo also prohibits customers from invading the privacy or harming other users.[321]

313 Vodafone Group Statement of Commitments to CEO Coalition to 'Make the Internet a Better Place for Children'. January 2013. p. 8. http://ec.europa.eu/information_society/newsroom/cf/document.cfm?doc_id=1655

314 Vodafone Group Statement of Commitments to CEO Coalition to 'Make the Internet a Better Place for Children'. op cit. p. 6. and Customer Protection: Keeping children safe. Vodafone UK. http://www.vodafone.co.uk/our-responsibilities/protecting-our-customers/customer-protection/

315 Airtel India. Terms and Conditions for Providing Services. Section 15.5.2. op. cit.

316 Airtel Kenya. Terms & Conditions for the use of Airtel Data. Section 5 (a) op. cit.

317 Safaricom. Conditions of Use for the Safaricom Prepaid Services. Section 6. http://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/conditions_of_use_for_the_safaricom_prepaid_services.pdf

318 Terms and Conditions: Content control. Vodafone. http://www.vodafone.co.uk/about-this-site/terms-and-conditions/content-control/ (Accessed 25 June 2014.) "Vodafone Group Statement of Commitments to CEO Coalition to 'Make the Internet a Better Place for Children," op. cit.

319 Allgemeine Geschäftsbedingungen für Vodafone-Dienstleistungen (AGB). Section 6.5. Vodafone Germany. http://www.vodafone.de/infofaxe/203.pdf

320 CONTRATO DE ADESÃO AO SERVIÇO VIVO INTERNET MÓVEL PÓS PAGO, op. cit. section 5.1, (g) and (h)

321 Ibid. Section 5.1a

Implementation in national context:

ISPs filter a broad range of content types in response to government requests or in compliance with the law. In the countries covered by this case study, typical types of content filtered by ISPs based on government order or legal mandate include what are deemed to be copyright-infringing materials, pornography, child-abuse images, defamation, hate speech, election-related speech and materials sensitive to national security. (See Chapter 2 for a discussion of how different states take different regulatory approaches to different content types.) Self- and co-regulatory efforts involving ISPs varied widely depending on national context. Case study researchers identified the following points of vulnerability for freedom of expression that ISPs and individuals face:

Obstacles to challenging government filtering requests

For ISPs, loss of operating license can result in unacceptably high costs to a business, especially where they invest in physical facilities, install equipment and hire large numbers of local staff in order to provide service in a given jurisdiction. In general, license agreements and the law vastly limit the choices available to ISPs when it comes to challenging government filtering requests. This includes decisions about: 1) whether or not to comply with a requests; 2) the type of public notice and explanation of the restriction provided by the service provider; and 3) whether and when to remove filters on particular content.

However, Vodafone's Disclosure to Law Enforcement Report underscores that Vodafone did challenge requests that were clearly not legal despite the risk of criminal liability and losing operating licenses.[322] None of the other companies studied for this research have made a similar public revelation.

Technical capacity and clarity of laws

In Brazil, research has shown that the most common type of restriction is carried out against defamatory content.[323] However most restrictions are targeted at the platform level (search engines, social networks, web-hosting services, etc.) instead of at the ISP network level. In fact, with the passage of the Marco Civil da Internet in 2014, ISPs are now forbidden from blocking, monitoring, filtering or analyzing online content.[324] Prior to 2014, Brazilian ISPs were rarely ordered to implement filtering by the government and regulations did not compel them to install software enabling the targeted restriction of specific content or pages. Because the ISPs lacked the technical means to carry out targeted filtering, filtering orders meant to restrict specific defamatory material on YouTube and the blog-hosting platform WordPress resulted in the entire services being blocked for

322 Vodafone Law Enforcement Disclosure Report. op. cit.
323 "Ameaças na Rede. Relatóriio de violações contra blogueiros, donos ou editores de site e usuários na internet em 2012. Article 19, 2013. p. 13. http://artigo19.org/wp-content/uploads/2014/01/RELAT%C3%93RIO-BLOGS-_Vers%C3%A3o-internet.pdf
324 Isabel Costa Carvalho, et. al. op cit.

short periods of time in 2007 and 2008 respectively.325 Now with the prohibition of ISP filtering, legal liability and enforcement in Brazil targets only the platform level, which will be the subject of further discussion in the case study examining social networking services.

In Kenya, no nationwide filtering has been reported, although in January 2013 researchers from the Citizen Lab at the University of Toronto in Canada identified the existence of a technology called PacketShaper, manufactured by a US company called BlueCoat, on Kenyan networks. Thus, while Kenyan ISPs have not apparently used PacketShaper's filtering capabilities, it appears that Kenyan authorities if not ISPs themselves possess the technical capability to carry out targeted filtering of content and web pages.[326]

Sometimes laws are only partially or unevenly enforced – or complied with to different degrees by different ISPs. In 2009, an Egyptian administrative court ordered the blocking of access to online pornography.[327] Initially, the order was not complied with, and in 2012 the Prosecutor General of Egypt ordered government ministries to enforce the ban.[328] As of 2013, news items reported that the National Telecom Regulatory Authority of Egypt announced the development of filtering software to prevent pornography from being shared, while as of January 2013 it has been reported that ISPs had installed filtering software on their networks.[329] In August 2013 the Administrative Court had ruled against the pornography ban, but meanwhile as per the media reports, the filtering software was already installed.[330]

Extension of "family friendly" filtering to adults by default

In 2014 the UK Government reached an agreement with four major British ISPs in which the companies will, as a self-regulatory scheme, offer customers 'family friendly network filtering services' that are automatically switched 'on' at the time of purchasing a broadband connection. In July 2014, Ofcom, the British telecommunications regulator published a report explaining that it is an 'unavoidable' choice for users to have filters

---

325 Brazil court orders ISPs to block access to Wordpress blog. OpenNet Initiative. 10 April 2008. https://opennet.net/blog/2008/04/brazil-court-orders-isps-block-access-wordpress-blog and YouTube Does Brazil. OpenNet Initiative. 10 January 2007. https://opennet.net/blog/2007/01/youtube-does-brazil (Accessed 9 April 2014.)

326 Appendix A: Summary Analysis of 'Countries of Interest.' In Morgan Marquis Boire, Jakum Dalek, and Sarah McCune, et. al. Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. Research Brief Number 13, January 2013. The CitizenLab. p. 25. https://citizenlab.org/2013/01/appendix-a-summary-analysis-of-blue-coat-countries-of-interest/ (Accessed 9 April 2014.) and The Right To Privacy in Kenya. Universal Periodic Review Stakeholder Report: 21st Session, Kenya. https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/upr_kenya.pdf

327 Egypt. Country report. OpenNet Initiative. 6 August 2009. https://opennet.net/research/profiles/egypt

328 Eva Galperin. Egyptian Prosecutor Orders Ban on Internet Porn. Electronic Frontier Foundation. 7 November 2012. https://www.eff.org/deeplinks/2012/11/egyptian-prosecutor-orders-ban-internet-porn (Accessed 10 April 2014.)

329 Egypt ready to block porn websites: Official. The Siasat Daily. 1 April 2013. http://www.siasat.com/english/news/egypt-ready-block-porn-websites-official (Accessed 10 October 2014.)

330 Al-Sayed Gamaleddine. Egypt court rules against banning porn websites. 24 August 2013. http://english.ahram.org.eg/NewsContent/1/64/79783/Egypt/Politics-/Egypt-court-rules-against-banning-porn-websites--.aspx (Accessed 10 April 2014.)

turned on at the time of purchase – while existing customers can 'opt in' to the scheme. Common categories of content to be filtered include suicide, self-harm, pornography and file sharing. Some ISPs also include content related to: alcohol, tobacco, dating, games, gambling, hacking, nudity, sexual education, social networking, media streaming, fashion, and search engines and portals.[331] In the media, the scheme has been justified as a means of protecting children from the harmful effects of pornography, but it has also been criticized in the media for having been implemented without public consultation and as a means for the UK Government to filter content that it does not want the public to access, including file sharing and extremist sites.[332]

'Collateral' Filtering

Overbroad or inconsistently applied laws can result in the inconsistent application of filtering within a country as well as the filtering of entire websites instead of specific infringing content within those websites, contradicting the 'necessary and proportionate' principle. Overbroad filtering is also known as 'collateral filtering' because of the collateral damage it can potentially inflict upon freedom of expression.[333]

In mid-2014, the NGO Open Rights Group tested the impact of Internet filters in the UK on nine different UK mobile and fixed line ISPs, and found that approximately one in five sites out of 100,000 tested are blocked by at least one of the ISPs.[334] The group encouraged users to send in personal reports about blocked websites: A young mother, for example, reported that an article to information about postpartum care was blocked. The political blog of a Syrian commentator was reported blocked by four services including Vodafone.[335]

In a recent ruling, the European Court of Justice held that ISPs could be required to filter access to websites that contribute to the infringement copyright, but that orders for filtering must be targeted. Specifically, the ruling stated, 'In this respect, the measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order

---

331 Ofcom Report on Internet safety measures - Internet Service Providers: Network level filtering measures. Ofcom. 22 July 2014. http://stakeholders.ofcom.org.uk/internet/internet-safety-2?utm_source=updates&utm_medium=email&utm_campaign=filtering-report

332 At the time of writing, there was a campaign to introduce filtering to restrict access by children to pornography. For more information see: Laurie Penny. David Cameron's internet porn filter is the start of censorship creep. The Guardian. 2 January 2014. http://www.theguardian.com/commentisfree/2014/jan/03/david-cameron-internet-porn-filter-censorship-creep (Accessed 10 July 2014.); Also see Warwick Ashford. UK internet porn filters a failure, says Open Rights Group. Computer Weekly. 3 July 2014. http://www.computerweekly.com/news/2240223883/UK-internet-porn-filters-a-failure-says-Open-Rights-Group (Accessed 10 July 2014.)

333 Nart Villeneuve. January 2006. The Filtering Matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace. First Monday. Vol. 11. No. 1-2. http://firstmonday.org/ojs/index.php/fm/article/view/1307/1227

334 Pam Cowburn. ORG's Blocked project finds almost 1 in 5 sites are blocked by filters. Open Rights Group. 2 July 2014 https://www.openrightsgroup.org/blog/2014/blockedproject%20 (Accessed 10 July 2014.)

335 Blocked! The personal cost of filters. Open Rights Group. July 2014. https://www.blocked.org.uk/personal-stories

to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued'.[336]

In India, civil society, the media, and government authorities have engaged in lively debates about the collateral impact of filtering, which ISPs are required to carry out upon receipt of a court order or instructions from an authorized government body. In 2013, the Indian Computer Emergency Response Team – the government branch broadly responsible for cybercrime located in the Department of Electronics and Information Technology – and the Department of Telecommunications (DoT), in response to a court order issued by the Gwalior district court, ordered the filtering of 78 URLs containing content related to the Indian Institute of Planning and Management.[337] Other authorities in the government's Department of Electronics and the government have publicly stated that they will contest the court order. According to journalists the petitioner argued that unblocking any of the links would constitute contempt of court.[338] The filters were criticized in the media as being overly broad and restricting legitimate speech; even a public notice issued by the University Grants Commission was filtered.[339] Also in 2013, the DoT, in response to a court order from the Supreme Court of India, issued an order to ISPs for the filtering of 39 websites that allowed users to share content - including pornographic content.[340] In addition to file sharing and image hosting websites, the URL shortening and ad hosting website Ad.fly was also filtered.[341] The potential for overly broad filtering in response to copyright laws has also been raised as a concern. For example, in 2011 Indian ISPs were found to filter entire file-sharing websites rather than specific URLs when acting on a court order to prevent piracy of a film called *Singham*. a 2011 film whose disparaging comments about Karnataka residents was exploited for violent protests.[342]

---

336 European Court of Justice. Judgment of the Court in Case C-314/12. 27 March 2014. para 56,. Mackinnon v Barr. Case C-123/12. 6 June 2014. http://curia.europa.eu/juris/document/document.jsf?text=&docid=149924&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=163325.

337 The Financial Express. After Court Order, DoT blocks web links critical of IIPM. 16 February 2013. http://www.financialexpress.com/news/after-court-order-dot-blocks-78-web-links-critical-of-iipm/1075073 (Accessed: 9 September 2014.)

338 Liat Clark. ISPs must block defamatory sites in India, including government's own pages. 19 Febuary 2013. http://www.wired.co.uk/news/archive/2013-02/19/india-government-sites-blocked (Accessed 26 June 2014.)

339 Shubhra Rishi. All Indian Enterprises should be Very Worried: Centre for Internet and Society. 25 February 2013. http://www.computerworld.in/feature/%E2%80%9Call-indian-enterprises-should-be-very-worried%E2%80%9D-centre-internet-and-society-75742013 (Accessed 26 June 2014.)

340 DNA. Govt orders Internet service providers to block 39 websites hosting obscene content. 26 June 2013. http://www.dnaindia.com/india/report-govt-orders-internet-service-providers-to-block-39-websites-hosting-obscene-content-1853550 (Accessed 26 June 2014.)

341 Softpedia. India Blocks 29 Adult Content and File Sharing Sites, Including Adf.ly. 1 July 2013. http://news.softpedia.com/news/India-Blocks-39-Adult-Content-and-File-Sharing-Sites-Including-Adf-ly-364750.shtml/ (Accessed: 26 June 2014.)

342 Apar Gupta. The Great Singham Filesharing Block. *India Law and Technology Blog*. 24 August 2011. http://www.iltb.net/2011/08/the-great-singham-filesharing-block/ (Accessed 26 June 2014.); NDTV. Singham effect: File sharing sites blocked. 22 July 2011 http://www.ndtv.com/article/india/singham-effect-file-sharing-sites-blocked-121249 (Accessed 26 June 2014.); 'Singham' Dialogue Offends Kannadigas. 23 July 2011. *DNA India*. www.dnaindia.com/entertainment/report-singham-dialogue-offends-kannadigas-1568545 (Accessed 13 August 2014.)

Transparency and Accountability of enforcement

Self-regulatory measures in the form of 'family friendly' filters made available by ISPs to users on their personal connection can risk placing the service provider (as well as the companies that sell filtering software to the ISPs) in the combined role of judge, jury and police: the ISP is responsible for determining the criteria to be included in the filter, implementing the filter, and addressing complaints about mis-categorized websites. The ISPs may in cases do this as part of their right to set private terms of reference, or in other cases, be acting in terms of a co-regulatory agreement made with the government. According to a representative from an NGO in the UK on the topic of the filters 'The government is encouraging companies to put in filters. But it is not clear how real the choice will be to opt out and avoid these filters, nor is it clear how filtering takes place. The government should not be allowed to promote such wide-ranging filtering without proper democratic scrutiny'.[343] Given the availability of software filters that parents can control on their own home networks, international experts such as the UN Special Rapporteur on freedom of expression Frank La Rue have questioned why ISPs should be legally required to filter content, calling government-mandated filtering 'difficult to justify'.[344]

The UK Government has also been criticized for seeking to expand the scope of self-regulatory efforts to other forms of content. As required by the Terrorism Act 2006, ISPs must, on request, filter or otherwise make unavailable websites and content that promotes terrorism.[345] In 2011, the UK Government sought the creation and implementation of a 'national block list' of extremist content and promoted the filtering of internet in libraries, schools etc.[346] According to news reports, between 2008 and 2011 the government implemented a pilot project in which illegal sites related to terrorism were blocked in schools and libraries. Critics have raised concern about lack of transparency and accountability throughout the process.Allegedly, sites were identified by the government's Counter Terrorism Internet Referral Unit (CTIRU), sent to the Crown Prosecution Services for vetting for compliance with the UK Terrorism Act 2006, and then shared with filtering software companies who then shared the filters with the libraries and schools.[347]

On the other hand, for certain types of content, such as hate speech, self-policing and self-regulation are sometimes viewed as more conducive to upholding freedom of expression compared to direct regulation and legal enforcement. A 2010 consultation by the OSCE Office for Democratic Institutions and Human Rights concluded that it is more

---

343 Phone interview conducted with Gabrielle Guillemin of Article 19 on 15 April 2014.
344 A/HRC/17/27. p.9
345 S2 and S3 of the UK Terrorism Act 2006. http://www.legislation.gov.uk/ukpga/2006/11/contents
346 The Prevent Strategy: What it means for library and information professionals. Briefing Paper. Chartered Institute of Library and Information Professionals. 20 January 2012. http://www.cilip.org.uk/sites/default/files/documents/Prevent%20strategy%20briefing%20Jan%202012.pdf
347 Jane Fae. The internet censorship programme you're not allowed to know about. politics.co.uk. 27 March 2014. http://www.politics.co.uk/comment-analysis/2014/03/27/the-internet-censorship-programme-you-re-not-allowed-to-know (Accessed 20 July 2014.)

effective for ISPs to restrict hate speech as measures to enforce their terms of service, instead of relying on the criminal justice system.[348]

Nonetheless there are concerns about delegating too much enforcement to private intermediaries. In an interview, Markus Löning of the research institute Stiftung Neue Verantwortung noted that these deliberations were 'more difficult' for 'certain types of pornography or hate speech'. Acknowledging that all ISPs may take down content according to their terms and conditions, he maintained that ISPs should delete illegal content under the aegis of and in cooperation with law enforcement. To illustrate, 'in the case of Nazi propaganda…it is the service provider's responsibility to work with prosecutors and law enforcement agencies, which means making a decision via a third instance'.[349]

Relationship between self-regulation, state regulation and law

Sometimes measures that begin as self-regulatory schemes can later be turned into regulation, or legislators can seek to formalize them in the law. In Kenya, in reaction to the post-election violence in 2007, Safaricom developed a number of self-regulatory guidelines to ensure that during election periods, content on the network is 'peaceful'. In 2012, Safaricom developed 'Guidelines for Political Mobile Advertising on Safaricom's Premium Rate Messaging Service', under which anyone intending to send bulk SMS of a political nature would first have to submit an application to Safaricom, and the company would vet the content to ensure that hate speech was not included.[350] These measures ultimately resulted in the development of regulatory guidelines by the Communications Authority of Kenya for the prevention of transmission of undesirable bulk political content via SMS.[351]

In June 2014, members of the UK parliament presented an 'Online Safety Bill'[352] requiring ISPs to withhold 'adult content',[353] and requiring users to prove that they are 18 years of age to opt in to access content.[354] This would change what are now self-regulatory measures by ISPs into formal legal requirements to filter 'adult content'.However, it is

348 Joe McNamee. The Slide From 'Self Regulation' to Corporate Censorship. European Digital Rights. January 2011. p. 29 http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf

349 Markus Löning, Director of the Privacy Project at Stiftung Neue Verantwortung Berlin and former German Federal Commissioner for Human Rights Policy and Humanitarian Aid. Interview with Kirsten Gollatz. Personal interview. Berlin, Germany, 7 April 2014.

350 Lucy Purdon. Corporate Responses to Hate Speech in the 2013 Kenyan Presidential Elections. Case Study: Safaricom. Institute for Human Rights and Business, in Digital Dangers: Identifying and Mitigating Threats in the Digital Realm (November 2013) p. 24. www.ihrb.org/pdf/DD-Safaricom-Case-Study.pdf.

351 Guidelines for the Prevention of Transmission of Undesirable Bulk Political Content/Messages via Electronic Communications Networks. CCK. September 2012. http://216.154.209.114/regulations/downloads/Guidelines_for_the_prevention_of_transmission_of_undesirable_bulk_political_content_via_sms.pdf

352 Online Safety Bill. HL Bill 19 55/3. 14 May 2013. http://www.publications.parliament.uk/pa/bills/lbill/2013-2014/0019/14019.pdf

353 Defined in the Bill as: 'harmful and offensive materials from which persons under the age of eighteen are protected.'

354 Online Safety Bill (amended). HL 16 55/4. 10 June 2014. http://www.publications.parliament.uk/pa/bills/lbill/2014-2015/0016/15016.pdf

important to note that this is a Private Members' Bill, meaning that there is very little chance of actually becoming law.[355]

BOX: Emerging Issue: 'Upstream Filtering'

Internet service providers and the practice of 'upstream filtering' can hinder freedom of expression. **As companies begin to practice filtering in one jurisdiction, other jurisdictions served by the provider can be affected by these practices. This is a result of the 'passing on' of any filter (or other technical component) in place on the ISP's network. This is known as upstream filtering, and the result is that content considered illegal in one jurisdiction and subsequently restricted, is continued to be restricted in another jurisdiction, where it might not be illegal.[356] For example, highlighting the importance of agreements and arrangements between ISPs – foreign and domestic – Citizen Lab of the University of Toronto reported in 2012 that the traffic peering arrangement Airtel India and Omantel led to a situation where Airtel India's content filters were also effective on the Omantel network in Oman.[357]**

3.2.2 Service Shutdowns and restriction

Governments can order network shutdowns or restrict internet services at a regional or national level. The restriction can affect the entire network or a specific service. Network shutdowns and service restrictions can be carried out for reasons related to the prevention of terrorism, the maintenance of public order and the prevention of public unrest. In many jurisdictions, ISPs must legally comply with such orders or risk legal penalty. They can also restrict or shut down the network or a service for the reasons of maintenance or technical failure.

The shutdown of an entire network or restriction of a service in a large area is a broad stroke that impacts all content, and is a restriction on freedom of expression that strongly risks not meeting internationally recognized principles such as proportionality and necessity.[358] Other more narrowly-targeted measures can also be taken. For example, a user's service can be terminated or suspended and the user will be unable to access the internet or use mobile services. Governments may issue orders for such termination or suspension of services. ISPs may also terminate or suspend a user's service or curtail access as a measure to enforce their own private policies.

Mobile telecommunications companies also receive orders from governments requiring them to send messages via their networks. This can affect freedom of expression, especially if the messages are not sent out in the government's name, because such measures 'push' certain information to users even if they do not restrict information.

---

355 Chris Davies. 16 May 2013. Private members' bills: Which ones made it from 2012? *BBC News*. www.bbc.com/news/uk-politics-22365004 (Accessed 14 August 2014.)

356 Chris Davies. 16 May 2013. Private members' bills: Which ones made it from 2012? *BBC News*. www.bbc.com/news/uk-politics-22365004 (Accessed 14 August 2014.)

357 The Citizen Lab. Routing Gone Wild: Documenting upstream filtering in Oman via India. 12 July 2012. https://citizenlab.org/2012/07/routing-gone-wild (Accessed 25 June 2014.)

358 A/HRC/17/27. pg.8

Company Policies

Internet service providers generally only restrict the entire network for maintenance or reasons out of their control. Companies do suspend or terminate user accounts. Such measures appear to be in compliance with broader legal mandates, court orders, or as self or co-regulatory steps taken to address specific types of content or behaviour – such as copyright infringement.

Compliance with government requests: ISPs examined for this case study inform users that their individual account or the network can be restricted in compliance with governmental orders. Some, such as Airtel India, state that the service can be disrupted and/or discontinued, suspended, etc. in response to directions, regulations, and notifications from the Regulator, or in compliance with any regulation or policy or other statutory authority.[359] Safaricom will terminate access to users' post paid services if required to do so by any licensing, law enforcement, or regulatory authority. [360]

In its 2014 Law Enforcement Disclosure Report, Vodafone recognized that orders for network shutdown are received by the company, and that this is a power that governments typically exercise in times of emergency.[361] The report also noted that there were other possible types of actions, including prioritizing SIMs (designating certain 'VIP' phone numbers for priority service when the network is congested), shutting down particular services and ceding direct network control to governments.[362] Vodafone UK does not explicitly mention restricting the service or network based on orders from authorized authorities in their general terms and conditions, though Vodafone Germany notes that disruption of the services could be due to orders by authorized officials.[363] None of the companies studied in this research clarify in their terms whether they could be legally required to send out messages of a political nature.

Enforcement of private rules: The circumstances and the detail regarding when the service or the network could be affected as per company policy differed. Airtel India,[364] Vodafone UK,[365] Vodafone Germany[366] and Safaricom[367] note that this can take place due to technical error, maintenance or geographical conditions. Airtel India lists a number of additional instances including: combating fraud and sabotage, in times of civil disorder, military operation, or local emergency, if services are used in contravention of laws in force, and any other reason/cause found to be reasonable by the company.[368] Airtel

359 Airtel India. Terms and Conditions for Providing Services. sections 2.1.2.6, 2.1.2.7, 2.1.2.9. op. cit.
360 Safaricom. Post Paid Terms for Use. section 16(a). http://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/standard_terms_conditions_safaricom_postpay_service_v1_feb_2010_tracked.pdf
361 Vodafone Law Enforcement Disclosure Report. p.68.
362 Ibid.
363 Vodafone Germany. Allgemeine Geschäftsbedingungen für Vodafone-Dienstleistungen (AGB). section 2.2. http://www.vodafone.de/infofaxe/203.pdfhttp://www.vodafone.de/infofaxe/203.pdfhttp://www.vodafone.de/infofaxe/203.pdf
364 Airtel India. Terms and Conditions. op. cit. section 2.1.2.6, 2.1.2.7, and 2.1.2.9.
365 Vodafone UK. Terms and Conditions: General Terms. section 2.2. http://www.vodafone.co.uk/about-this-site/terms-and-conditions/general-terms/
366 Vodafone Germany., op.cit.
367 Safaricom. Safaricom Post Pay Customer Terms and Conditions. section 5. op. cit.
368 Airtel India. Terms and Conditions. op.cit. section 2.1.2.

Kenya broadly states that services might be terminated if Airtel is unable to continue to supply the services due to contractual, economical, or operational reasons.[369] Vodafone UK notes that the service might be affected to preserve network security, when there is Artificially Inflated Traffic, and during Emergency Planning Measures.[370] Vivo broadly states that the services can be affected if the authorization for the company to operate is withdrawn by the Government.[371]

All ISPs reserve the right to terminate, suspend, or moderate the service for abuse of the service or breach of the company Terms and Conditions. Beyond this, Airtel India reserves the right to terminate or suspend accounts for the same reasons as noted above, while Airtel Kenya specifies that any violation of the provisions for 'User Conduct' will result in account termination.[372] Safaricom, for post-pay services, reserves the right to terminate services if the company believes that the Service is being used in an unauthorised or illegal way or for criminal activities.[373] Safaricom may suspend or disconnect those who use its services 'in an unauthorised, unlawful, or fraudulent manner' or if the communications are 'illegal, a nuisance, abusive, a hoax, menacing or indecent'. The conditions of use clearly state that the 'SIM Card will at all times remain our property'[374] Vodafone UK reserves the right to terminate services if the company reasonably believes that the equipment or services are being used for purposes that are abusive, a nuisance, illegal, or fraudulent.[375]

Implementation in national context

ISPs are faced with difficult decisions about how to comply, and how to communicate with the public about their compliance. Below are some specific examples.

Nationwide shutdowns

Government orders to shut down all internet services for an entire nation are rare. During the 2011 Egyptian Revolution, the government shut down mobile and Internet networks for the entire country from 28 January to 2 February 2011.[376] According to some experts, the shutdown that occurred in Egypt was unprecedented in its scope.[377] Journalists further explain that the shutdown was possible, in part, because of the structure of Egypt's

369 Airtel Kenya. Terms & Conditions for the use of Airtel Data. op. cit. section 10.
370 Vodafone UK. Terms and Conditions: General Terms. section 2.2 http://www.vodafone.co.uk/about-this-site/terms-and-conditions/general-terms/
371 Vivo. Contrato De Adesao Ao Servico Vivo Internet Movel Pos Pago. section 9(e). http://www.vivo.com.br/consumo/groups/public/documents/documentopw/ucm_009621.pdf
372 Airtel Kenya. Terms & Conditions. op. cit. section 5.
373 Safaricom. Safaricom Post Pay Customer Terms and Conditions. op. cit. section 16(a).
374 Ibid. section 5.
375 Vodafone UK. Terms and Conditions. op. cit. section 3.3(a).
376 Christopher Roads and Geoffrey Fowler. Egypt Shuts Down Internet, Cellphone Services. 29 January 2011. http://online.wsj.com/news/articles/SB10001424052748703956604576110453371369740 (Accessed 20 July 2014.)
377 According to a news interview with the network security firm Renesys Corp, other countries like Iran, Tunisia, and China exert control over the internet – but this is via methods such as blocking particular websites and slowing down the internet. Egypt's case is unique as within 20 minutes all of the largest service providers in Egypt were shut down. Larry Greenemeirer. How Was Egypt's Internet Access Shut Off?. Scientific American. 28 January 2011 http://www.scientificamerican.com/article/egypt-internet-mubarak/ (Accessed 7 July 2014.)

telecom sector: most ISPs are licensees of the state telecom – making them legally bound to the Orders and Rules of the Telecommunication Regulatory Authority.[378] Vodafone, one of the many ISPs that received the order, shut down its network.[379] Following the shutdown, the Vodafone Group published a statement explaining why the company complied with the requests.[380]

Service providers are not always clear in their terms of service that they will shut down the entire network, a particular service, or accounts if required to do so by legal mandate, though as of June 2014 Vodafone has clarified this possibility in their Law Enforcement Disclosure Report.[381] Prior to publication of that report, Vodafone was criticized for complying with the 2011 governmental orders related to network and service restrictions in Egypt.[382] In this context, human rights organizations questioned Vodafone's compliance with Egyptian authorities and asked that the company develop clear standards applicable to all its operations for responding and addressing such requests.[383]

Targeted and localized shutdowns

In 2012 the Government of Jammu and Kashmir, India, was reported in the media to have ordered a regional shutdown of mobile and internet service to prevent riots in response to the YouTube film 'Innocence of Muslims' for approximately a day.[384] Government officials in Jammu and Kashmir were cited in the news as stating that all Internet services were not shut down in the region, and Airtel India was cited as having carried the following message: 'Mobile Internet access is not available on your Airtel mobile today in compliance with an advisory from the Jammu and Kashmir Police.'[385] Note that the steps by the authorities to shut down service in Jammu and Kashmir came alongside an order to ISPs to block

378 Babu Kurra. Egypt Shut Down Its Net With a Series of Phone Calls. Wired. 28 January 2011. http://www.wired.com/2011/01/egypt-isp-shutdown/ (Accessed 7 June 2014.)

379 John Oates. Vodafone confirms Egypt lock-down. The Register. 28 January 2011. http://www.theregister.co.uk/2011/01/28/egypt_vodafone_shuts/ (Accessed 7 June 2014.)

380 Vodafone Group Plc – Response on Issues Relating to Mobile Network Operations in Egypt. 22 February 2011. http://www.business-humanrights.org/media/documents/vodafone-statement-re-egypt-22-feb-2011.pdf (Accessed 7 June 2014.)

381 Vodafone Law Enforcement Disclosure Report. p.68.

382 Telco Hall of Shame: Vodafone. Access Blog. 29 January 2013. https://www.accessnow.org/blog/2013/01/29/hall-of-shame-vodafone (Accessed 10 June 2014.)

383 Juliette Garside. Vodafone under fire for bowing to Egyptian pressure. The Guardian. 26 July 2011. http://www.theguardian.com/business/2011/jul/26/vodafone-access-egypt-shutdown (Accessed: 7 July 2014.)

384 Note: Jammu and Kashmir is not the only region that has ordered the blocking of the film 'Innocence of Muslims'by restricting access to content or the network.

385 Pamposh Raina and Betwa Sharma. Telecom Services Blocked to Curb Protests in Kashmir. The New York Times. 21 September 2012. http://india.blogs.nytimes.com/2012/09/21/telecom-services-blocked-to-curb-protests-in-kashmir/ (Accessed 26 June 2014.)

access to YouTube and Facebook in the region.[386] This is, in an example of how shutdown orders are sometimes accompanied by orders for filtering.[387]

BOX: Bypassed legal procedure in 2005 O2 localized network shutdown

In 2005, the City of London Police implemented a localized service restriction by 'switching off' parts of O2's network 1km around the Aldgate Station after the terrorist bombings in London.[388] The shutdown lasted from 12.00 pm to 4.45 pm. The request to O2 to give privileged access to its network to emergency services, and restrict it to others – known as 'Access Overload Control' (ACCOLC) – was issued by the London Police because they were having difficulty communicating in the Aldgate area. This was done despite the fact that the Gold Co-ordinating Group, which is administratively responsible for authorizing network shutdowns, decided not to shut down the networks and activate ACCOLC.[389] According to London Assembly's 7 July Review Committee report of the bombings, during the shutdown it was estimated that possibly over a million individuals' communications were impacted.[390] The 7 July Review Committee also found that there was a need to review and restructure the protocol to be followed during emergency circumstances to ensure authorities are provided with adequate and effective procedures to follow.[391] Note that the order for restriction was only for O2's network.

Government requirements for specific messaging, or restriction of messaging, in times of crisis. During the 2011 protests, the Egyptian Government not only shut down mobile and internet networks, but required ISPs including Vodafone to send political messages from the authorities.[392] Later in a public statement Vodafone clarified that Vodafone had declined to send the messages in the company's name and insisted that the messages clearly and accurately attribute the governmental department sending the message.[393]

In India, in 2012, in response to sectarian threats circulating in several cities in the wake of riots in the North Eastern state of Assam, in addition to other actions including orders for the blocking of content and suspension of accounts,[394] the government of India placed a temporary nationwide restriction on SMS and data, not allowing more than five SMSs or MMSs and no attachments over 25 KB of data to be sent per day for a period of

386 Riyaz Wani. J&K government blocks access to Facebook and Youtube. Tehelka. 1 October 2012. http://archive.tehelka.com/story_main54.asp?filename=Ws011012Jammu.asp (Accessed 26 June 2014.)
387 Ibid.
388 7 July phone shutdown criticized. BBC News. 1 March 2006. http://news.bbc.co.uk/1/hi/england/london/4763350.stm (Accessed 29 June 2014.)
389 London Assembly. Report of the 7th July Review Committee. p.44 June 2006. http://www.london.gov.uk/sites/default/files/archives/assembly-reports-7july-report.pdf
390 Ibid.
391 Ibid. p.47.
392 Amy Saunderson Meyer. 16 February 2011. 7 Lessons from the Egyptian Revolution. PBS: Idea Lab., http://www.pbs.org/idealab/2011/02/7-lessons-from-the-egyptian-revolution047/ (Accessed 30 May 2014.)
393 Vodafone Group Plc – Response on Issues Relating to Mobile Network Operations in Egypt. 22. Op.cit.
394 Pranesh Prakash. Analysing Latest List of Blocked Sites (Communalism Edition). The Centre for Internet and Society. 22 August 2012. http://cis-india.org/internet-governance/blog/analysing-blocked-sites-riots-communalism (Accessed 7 July 2014.)

fifteen 15 days.[395] Information about the restriction was initially reported in news items that cited confirmation of the restriction by the press office of Ministry of Home Affairs,[396] but a public statement from government could not be located during this research. News portals reported that Airtel India did not appear to have implemented the restriction, while users sending the 6th message via Chennai, India-based company Aircel, were met with the following message 'Due to Govt. directives, more than 5 SMS per day are blocked. Please retry tomorrow. Anticipate your co-operation'.[397] Earlier, in 2010, the Government of India also issued a temporary ban on all bulk SMS and MMS services. This restriction was announced via a government press release that noted the duration of the restriction and the governmental departments responsible for the restriction.[398]

In 2008 the Kenyan government initially considered shutting down SMS services during the election period, in response to the 2007 post-election violence that occurred in the region. As an alternative, Safaricom arranged with the Kenyan Government to have service providers send messages of 'peace and calm' to users on their own initiative and in the name of the company.[399]

Suspension, termination or curtailment of specific user accounts.

In Kenya, in compliance with the 2013 law requiring individuals to register SIMs with government identification, service providers including Safaricom[400] and Airtel Kenya[401], suspended services to unregistered subscribers. In countries across the European Union, courts have ordered service providers to disconnect users engaging in file sharing of copyright infringing material.[402] In the UK, as of mid-2014, the Digital Economy Act 2010 (DEA) required ISPs to temporarily suspend the accounts of users persistently downloading copyrighted material, though the lack of enabling legislation meant that these provisions had not been put into effect.[403] In 2012, some UK ISPs challenged the

395 Shreya Shah. India Bans Mass SMS to Counter Panic Wall Street Journal. 17 August 2012. http://blogs.wsj.com/indiarealtime/2012/08/17/indian-bans-mass-sms-to-counter-panic/ (Accessed 7 July 2014.)
396 Ibid.
397 Indian Government Imposes 5 SMS Per Day Limit for the Next 15 Days. Tech Gadgets Web. 18 August 2012. http://www.techgadgetsweb.com/10185/indian-government-imposes-5-sms-day-limit-15-days (Accessed 7 July 2014.)
398 Ban on Bulk SMS and MMS Extended. Ministry of Communications & Information Technology. 24 September 2010. http://pib.nic.in/release/rel_print_page.asp?relid=65982 (Accessed 7 July 2014.)
399 Alice Munyua. Kenya: Perceptions and Misconceptions: The Role of New and Traditional Media in Kenya's Post Election Violence. GIS Watch and Kenya ICT Action Network (KICTANet). 2011. http://www.giswatch.org/sites/default/files/gisw_-_kenya.pdf (Accessed 10 July 2014.)
400 Safaricom Limited Annual Report for the Year Ended 31 March 2013. Safaricom. p. 5. https://www.safaricom.co.ke/images/Downloads/Resources_Downloads/Annual_Report.pdf and Wanyama wa Chebusiri. Kenya's Battle to Switch Off Fake Phones. BBC News. 5 October 2012. www.bbc.com/news/world-africa-19819965 (Accessed 10 April 2014.)
401 Kenya: mobile operators switch off 2.4 million users' phones. IT News Africa. 15 January 2013. http://www.itnewsafrica.com/2013/01/kenya-mobile-operators-switch-off-2-4-million-users-phones/ (Accessed 10 April 2014.)
402 Miguel Peguera. Spanish Court Orders an ISP to Disconnect a Copyright Infringer. 22 January 2014. http://cyberlaw.stanford.edu/blog/2014/01/spanish-court-orders-isp-disconnect-copyright-infringer (Accessed 14 July 2014.)
403 Philip Ward. Digital Economy Act 2010: copyright. House of Commons Library. 28 June 2013. p.3. https://wiki.openrightsgroup.org/wiki/Digital_Economy_Act_2010

DEA's legality in the UK Court of Appeal, which upheld the Act.[404] However, in 2012 the codes that were intended to combat copyright infringement, drafted by Ofcom pursuant to the DEA, were withdrawn.[405] In July 2014, as a self-regulatory step, major ISPs in the UK, the government, and the music industry established the 'Voluntary Copyright Alert Programme', which sends warnings to infringing users pointing out their illegal behaviour and providing them with legal alternatives to access content. Notably, the programme does not impose sanctions such as disconnection. Furthermore, the government indicated that the relevant DEA provisions would be shelved.[406]

3.2.3 Network Neutrality

'Network neutrality' is the principle that ISPs should treat all data equally and not prioritize data or services for any reason – including commercial and political ones.[407] Net neutrality is important for freedom of expression because it preserves individual's choice and right to access internet content, applications, services and hardware.[408] ISPs have access to technologies that allow them to analyse, block or slow down content and services. These practices can threaten network neutrality. According to Barbara van Schewick of Stanford Law School's Center for Internet and Society and David Farber of Carnegie Mellon University, ISPs are motivated to discriminate against selected applications for economic reasons, bandwidth regulation and restriction of content. They recommend greater transparency by companies as to how their broadband services work, what types of network management activities they engage in, and how such activities might affect consumers.[409]

Across the jurisdictions studied in this research, governments and regulators are struggling to understand how and if network neutrality should be protected by law, and what responsibility companies should have in ensuring network neutrality. Brazil is the only country studied in this research that guarantees network neutrality by law. With the passage of the Marco Civil da Internet, ISPs are responsible for the transmission of data

404 Digital Economy Act not in breach of EU laws, Court of Appeal rules. Out-Law.com. 6 March 2012. http://www.out-law.com/en/articles/2012/march1/digital-economy-act-not-in-breach-of-eu-laws-court-of-appeal-rules/ (Accessed 10 August 2014.); R (on the application of (1) British Telecommunications Plc, (2) Talk Talk) v BPI Ltd and others [2012] EWCA Civ 232.

405 Digital Economy Act copyright regime shelved by UK government. Out-Law.com. Pinsent Masons. 24 July 2014. http://www.out-law.com/en/articles/2014/july/digital-economy-act-copyright-regime-shelved-by-uk-government/ (Accessed 13 August 2014.)

406 Mark Jackson. Update UK ISPs Agree to Voluntary Internet Piracy Warning Letters Scheme. ISP Review. 19 July 2014. http://www.ispreview.co.uk/index.php/2014/07/big-uk-isps-agree-voluntary-internet-piracy-warning-letters-scheme.html (Accessed 27 July 2014); Digital Economy Act copyright regime shelved by UK government. 24 July 2014. op. cit. (Accessed 13 August 2014.)

407 Barbara van Schewick. 6 May 2014. The Case for Rebooting the Network-Neutrality Debate. The Atlantic. http://www.theatlantic.com/technology/archive/2014/05/the-case-for-rebooting-the-network-neutrality-debate/361809/ (Accessed 13 August 2014.)

408 Freedom of Expression and ICTs: Overview of International Standards. Article 19. 2013. p.14. http://www.article19.org/data/files/medialibrary/37380/FoE-and-ICTs.pdf

409 Barbara van Schewick and David Farber. February 2009. Point/counterpoint network neutrality nuances. Communications of the ACM. Vol. 52 No. 2. http://www.thei3p.org/docs/events/WESIINetNeutrality2.pdf

regardless of content, ensuring that any traffic discrimination or degradation must be in accordance with law, providing to consumers clear notice of network traffic management and security practices, refraining from anti-competitive practices, and refraining from blocking, monitoring, filtering or analysing the content of data packets except as established by law.[410]

In the UK, Ofcom has published a statement on net neutrality that broadly exhorts companies to be transparent as and when internet traffic is managed, and recommending market-based solutions to problems that arise.[411] In 2013, UK broadband providers developed a voluntary industry code on traffic management transparency for broadband services, in which they have committed to treat all traffic equally while also providing users with accessible information about their respective traffic management practices. [412] In April 2014, the European Commission proposed changes to a number of regulations through the 'Connected Continent Legislative Package'. Among other things, the proposed regulation mandates net neutrality by prohibiting discriminatory blocking and throttling practices, defining clear rules and principles for traffic management, and requiring that specialized services must provide adequate and standard quality of internet service.[413] Though the proposed regulation originally allowed for the filtering of content for the purpose of implementing legal provisions, on a court order, or to prevent or impede serious crimes, it was later amended to permit filtering only on receipt of a court order.[414] In reaction to the proposal, some members of industry issued a joint statement criticizing the proposal as being 'restrictive, anti-innovation, and anti-consumer choice', the statement also critiqued the legislative process as being rushed and not based on adequate technical analysis.[415]

Concerns have also been raised by politicians in the UK that provisions relating to filtering in the regulation will have a negative impact and allow for content such as child abuse images to be shared.[416] In 2013, the German Government also proposed a law mandating network neutrality in reaction to a German ISP throttling services of customers who

---

410 Marco Civil da Internet. op. cit. Article 9, section (1),(2), (3).

411 Ofcom's approach to net neutrality. Ofcom. 24 November 2011. http://stakeholders.ofcom.org.uk/consultations/net-neutrality/statement/

412 Voluntary industry code of practice on traffic management transparency for broadband services. Broadband Stakeholder Group (UK). http://www.broadbanduk.org/wp-content/uploads/2013/08/Voluntary-industry-code-of-practice-on-traffic-management-transparency-on-broadband-services-updated-version-May-2013.pdf

413 Connected continent legislative package. Digital Agenda for Europe. https://ec.europa.eu/digital-agenda/en/connected-continent-legislative-package

414 Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/22/EC, and Regulations (EC) No 1211/2009 and (EU) No 531/2012. Article 23 paragraph 5. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0190+0+DOC+XML+V0//EN

415 Frances Robinson. Battle Lines Drawn Over Net Neutrality in Europe. Wall Street Journal Digits blog. 1 April 2014. http://blogs.wsj.com/digits/2014/04/01/battle-lines-drawn-over-net-neutrality-in-europe/ (Accessed 25 June 2014.)

416 Net neutrality law adopted by European Parliament. BBC News. 3 April 2014. http://www.bbc.com/news/technology-26865869 (Accessed 25 June 2014.)

exceed their monthly quotas. While the principle of net neutrality has been legally codified (§ 41a TKG) in Germany, it is still not entirely safeguarded through concrete provisions.[417]

Despite a number of jurisdictions proposing legislation, there still exist a number of regulatory gaps around net neutrality. Thus, practices vary from company to company. For example, even though India lacks formal legal provisions, it is believed that ISPs generally adhere to net neutrality.[418] However, in 2013 Airtel India and Google have received criticism for a joint venture known as 'free zone' that would allow Airtel India customers to access initial searches and email for free.[419] Similar options are offered to users in Kenya through services like Facebook Zero, which allow subscribers to access text versions of the service for free through collaborations between Facebook and ISPs.[420] In response to critics of 'free zones' there is a strong counter argument that these measures increase user choice and provide access to the internet to users who otherwise would not have access.[421]

3.3 Privacy

Service providers have access to a broad range of information about their subscribers including metadata, communications content, location, etc. According to the UN High Commissioner for Human Rights' report on the Right to Privacy in the Digital Age: 'Enterprises that provide content or Internet services, or supply the technology and equipment that make digital communications possible, for example, should adopt an explicit policy statement outlining their commitment to respect human rights throughout the company's activities. They should also have in place appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact. Companies should assess whether and how their terms of service, or their policies for gathering and sharing customer data, may result in an adverse impact on the human rights of their users'.[422] Further the report holds that 'even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association'.[423]

---

417 Iain Morris. German minister proposes net neutrality rules to rein in Deutsche Telekom: report. 17 June 2013. http://www.telecomengine.com/node/79864 (Accessed 25 June 2014.)

418 The Times of India. What is net neutrality and why is it important. The Times of India. 20 January 2014. http://timesofindia.indiatimes.com/tech/tech-news/What-is-net-neutrality-and-why-it-is-important/articleshow/29083935.cms (Accessed 16 April 2014).

419 Sudipto Sircar. Airtel Partners With Google: Latest Network Neutrality Violation. India Law and Technology Blog. 3 July 2013. http://www.iltb.net/2013/07/airtel-partners-with-google-latest-network-neutrality-violation/ (Accessed: 6 June 2014.)

420 David Talbot. 21 March 2013. Facebook and Google Create Walled Gardens for Web Newcomers Overseas. MIT Technology Review. www.technologyreview.com/news/512316/facebook-and-google-create-walled-gardens-for-web-newcomers-overseas (Accessed 13 August 2014.)

421 Tasneem Akolawala. Airtel and Google join hands to provide free internet for mobile users in India. DNA. 26 June 2013. http://www.dnaindia.com/scitech/report-airtel-and-google-join-hands-to-provide-free-internet-for-mobile-users-in-india-1853383 (Accessed 9 September 2014.)

422 A/HRC/27/37. p.15.

423 A/HRC/27/37. p.7.

3.3.1 Company Policies

This section provides a breakdown of how companies covered in this case study articulate their policies affecting users' privacy. It will be followed by a section analyzing the outcomes produced when those particular company policies interact with the policies, laws, and actions of specific governments.

General privacy practices: Vodafone Group has a comprehensive privacy policy that is applicable to its subsidiaries in different countries,[424] and has a number of supplementary policies that address user privacy including: the 'Global Policy Standard on Law Enforcement Assistance' and the 2014 Sustainability Report.[425] Vodafone UK and Airtel India have comprehensive privacy policies governing their data practices and refer to privacy in their Terms. Vodafone UK's privacy policy broadly addresses the collection, use, sharing and disclosure, security, and users rights with respect to personal information.[426] Vodafone UK's General Terms also clarify that the company is a data controller under the Data Protection Act 1998 and each party to the contract is bound to comply with the legal duties laid out in the Act.[427] Similarly, Vodafone Germany notes in its General Terms that the company handles users' personal data in compliance with the statutory provisions for data protection including the Telecommunications Act (TKG), the German Federal Data Protection Act (BDSG) as well as for the application of Internet services, the Telemedia Act (TMG).[428]

Airtel India's 'Online Privacy Policy' addresses what personal information is, when personal information will be collected, how it will be used, when it can be disclosed and transferred, security procedures and practices around personal information, how individuals can update their personal information, and how users can submit complaints or feedback to the company.[429] The Airtel India terms further note that the privacy of users' communications are subject to relevant laws and regulations.[430] On the other hand, Airtel Kenya does not appear to have a dedicated privacy policy, nor does Safaricom. This is reflective of the legal environment, as Kenya does not have a Data Protection Act. Despite this, Airtel Kenya touches upon privacy in its Terms for Airtel data, noting the circumstances under which the company will monitor, vet, edit or knowingly disclose the contents of emails. [431] Safaricom in its Terms of post- pay mobile services touches upon

---

424 Additionally, the parent company Vodafone Group has a thorough privacy policy applying to its subsidiaries. See: Vodafone privacy commitments. http://www.vodafone.com/content/index/about/about-us/privacy.html, and also: Privacy at the heart of Vodafone. http://www.vodafone.com/content/dam/vodafone/about/privacy/vodafone-privacy-programme.pdf

425 Sustainability Report 2013/14. Vodafone Group Plc. http://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf

426 Vodafone UK. Understanding our privacy policy. http://www.vodafone.co.uk/about-this-site/our-privacy-policy/

427 Vodafone UK. Terms and Conditions: General Terms.section 17.2. http://www.vodafone.co.uk/about-this-site/terms-and-conditions/general-terms/

428 Vodafone Germany. Allgemeine Geschäftsbedingungen für Vodafone-Dienstleistungen (AGB). section 9.1. http://www.vodafone.de/infofaxe/203.pdf

429 Airtel India. Online Privacy Policy. op. cit.

430 Airtel India, Terms and Conditions for Providing Services. Section 2.1.4. op. cit.

431 Airtel Kenya. Terms & Conditions for the use of Airtel Data. Section 7. op. cit.

the potential uses and circumstances for disclosure and sharing of users' personal and banking information.[432]

Vivo does not have a privacy policy that was publicly accessible at the time of this research and company representatives did not respond to requests for interviews. In June 2014, however, Vivo's parent Telefonica released a Sustainability Report announcing that 'the Group has a Privacy Policy approved by the Board in March 2013 which has to be complied with in all the countries in which we operate, and that the company had appointed a Chief Privacy Officer.[433] The report also states that the group has established 'common standards of behaviour for all our companies'. This includes a commitment to 'protect the confidentiality of personal information entrusted to us, whether that of customers, shareholders, employees or suppliers', and 'Inform users on how to access and correct the data we handle'.[434] Making privacy policies of specific services publicly available would be consistent with that commitment, and advocacy group Access has called on Telefonica to release specific details of the company's privacy policy, which its report implies adheres to globally consistent standards.[435]

Data Retention: Vodafone UK[436] and Airtel India,[437] which both have dedicated privacy policies for their services, maintain that the company retains subscriber information as legally required or for as long as necessary to provide customers with the service requested. Policies for the other companies studied were not publicly available. In Telefonica's sustainability report which also applies to Vivo, the company commits to 'provide our stakeholders with relevant information about how we use and store their personal data' although there are no publicly available details on how subsidiary brands such as Vivo carry out this commitment.[438]

Real-time surveillance and responding to government user data requests: ISPs can be analysed in terms of how they respond to governmental mandates for real time surveillance and access to user data with differing levels of clarity. For example, for its post-pay services, Safaricom reserves the right to hold and use information provided by the user for carrying out legal, governmental, or regulatory requirement in connection with a legal proceeding or in respect of crime or fraud prevention, detection or prosecution. The company can also monitor or record voice or data services in order to prevent or detect crime.[439] In the terms for Safaricom's pre-paid services, the company reserves the right to disclose, receive and record any details of the use of the services including, though not

---

432 Safaricom. Post Paid Terms for Use. section 11. op. cit.
433 Telefonica 2013 Sustainability Report. http://www.rcysostenibilidad.telefonica.com/wp-content/uploads/2014/07/Informe_Sostenibilidad2013_ENG3jul.pdf p. 126.
434 Ibid. p. 120.
435 Peter Micek and Ana Monteiro. Telefónica reports progress on privacy and free expression principles. 26 June 2014. Access blog. https://www.accessnow.org/blog/2014/06/26/telefonica-reports-progress-on-privacy-and-free-expression-principles (Accessed 18 July, 2014.)
436 Vodafone UK. Understanding our privacy policy. http://www.vodafone.co.uk/about-this-site/our-privacy-policy/
437 Airtel India. Privacy Policy: Security Practices and Procedures. http://www.airtel.in/forme/privacy-policy/security+practices+and+procedures?contentIDR=9346516c-c1a1-4bd7-bce0-6945236dceaa&useDefaultText=0&useDefaultDesc=0
438 Telefonica 2013 Corporate Sustainability Report. op. cit. p. 120.
439 Safaricom. Post Pay Terms and Conditions. Section 11.3 (a) and (b), op.cit.

limited to calls, emails, SMSs, data, personal information or documents obtained from the user for the purposes of fraud prevention and law enforcement, reasonable commercial or business purposes, in compliance with legal, governmental or regulatory requirement and for use by lawyers in connection with any legal proceedings.[440] This standard does not clarify to the user if and how the company complies with real time surveillance requests or if the company provides access to historical data collected and stored by the company.

On the other hand, as noted above, Airtel India broadly references that the privacy of communications is subject to compliance with relevant laws and licenses, which would include legal provisions pertaining to surveillance,[441] while noting specific instances that they will share information with law enforcement or government agencies in their Online Privacy Policy.[442] Airtel Kenya discloses email content if it is legally required.[443]

Of all the companies studied, the Vodafone Group was the only ISP that published a comprehensive policy on responding to demands from authorized authorities. Vodafone's policy is known as the 'Global Policy Standard on Law Enforcement Assistance' and includes information about its process for evaluating and responding to requests for user data from law enforcement. The policy specifies that Vodafone is bound to the laws of the jurisdiction in which it operates, and that the company engages with governments to protect user rights to the extent possible.[444] Furthermore, Vodafone's 2014 Law Enforcement Disclosure Report sheds light on the complex situation that ISPs face when complying with requests from authorized authorities – pointing to the challenges of evolving technology, opaque law, and secrecy requirements. Vodafone also clarifies in the report that the company collaborates with authorized authorities in three ways: response to legal requests, voluntarily in clear emergency situations (such as a kidnapping) and proactively to protect the Vodafone network.[445]

Telefonica's Sustainability Report, which by extension is applicable to its subsidiary company Vivo, states, 'Telefonica has formal processes for handling data requests from local or governmental authorities. These processes are the responsibility of the departments of the General Secretary and Security in each Group company'.[446] The company also reports that in 2012 it carried out a human rights impact assessment with the assistance of the non-profit consultancy Business for Social Responsibility (bsr.org). Its report further states that 'the exercise carried out allowed us to identify privacy and freedom of expression as high-risk aspects for the sector; in search of a global solution

440 Ibid.
441 Airtel India. Terms and Conditions for Providing Services. op. cit. Section 2.1.4.
442 Airtel India. Privacy Policy. http://www.airtel.in/forme/privacy-policy/disclosure+and+transfer?contentIDR=745792ad-d6af-4684-85d4-d85773e77356&useDefaultText=0&useDefaultDesc=0
443 Airtel Kenya. Terms & Conditions for the use of Airtel Data. Section 7. op. cit.
444 Note: The policy states that Vodafone may be bound to follow laws that are overly restrictive, and thus Vodafone's actions may consequently be overly-restrictive. However, Vodafone does indicate that it engages in advocacy with governments to bring about changes in restrictive laws. See: Vodafone. Human Rights and Law Enforcement. op. cit.
445 Vodafone. Law Enforcement Disclosure Report. op. cit.
446 Telefonica 2013 Sustainability Report. op. cit. p. 126

we helped to create the [Telecommunications Industry] Dialogue Group on Freedom of Expression and Privacy'.[447]

Identification practices: The ISPs studied in this research comply with legal requirements for the registration of subscribers via government-issued identification. For example, Airtel India,[448] Airtel Kenya[449] and Safaricom[450] require users to submit government-issued identification. Even when ISPs are not legally required to collect government identification from subscribers, many do verify provided information at the time of signing service contracts. In Brazil, users are required to register with their real names before purchasing a mobile phone or subscribing to a private internet connection.[451] In Germany, although paragraph 111 of the Telecommunications Act requires suppliers of SIM cards to verify a customer's identity from customers, this is not rigorously enforced in practice and suppliers do not check on the accuracy of the information provided upon activation so it remains possible for people to obtain SIM cards anonymously.[452]

3.3.2 Implementation in national context

Below is an examination of how the company policies described above play out in specific national contexts.

Compliance with government requests and legal mandates

Vodafone's Disclosure to Law Enforcement Report does more than any other ISP to shed light on the challenges companies face in respecting users' privacy. The report describes the range of legal requirements that the company faces around the world – including requirements that directly violate user privacy – such as the requirement to provide authorities in a number of jurisdictions with a direct line of access into the company network. In a strong move towards protecting user privacy, Vodafone has called on governments to amend legislation that allows government agencies and authorities to gain direct access to an ISP's infrastructure, and to take steps to discourage agencies from seeking direct access without legal authorization.[453]

---

447 Telefonica 2013 Sustainability Report. op. cit. p. 126

448 According to the Department of Telecommunications Revised Guidelines on Verification of New Mobile Subscriber for post paid and pre paid, users must submit a passport sized photograph, proof of identity, and proof of address. This information must be verified by Airtel. Airtel notes that it will carry out verification of subscriber information in Section 1.4 of Airtel India. Terms and Conditions for Providing Services. op. cit.

449 Airtel Kenya. Customer Registration page. http://africa.airtel.com/wps/wcm/connect/africarevamp/Kenya/home/customer-care/Customer-registration/

450 Safaricom. Subscriber SIM Registration Form. http://www.safaricom.co.ke/about-us/subscriber-registration/subscriber-registration.html

451 Freedom House. Freedom on the Net - Brazil – 2013. http://www.freedomhouse.org/report/freedom-net/2013/brazil

452 L. Sobiraj. Datenschutz: Die Crux mit den anonymen Prepaid-Karten [Data Protection: the crux with anonymous prepaid cards]. 18 August 2013. teltarif.de. http://www.teltarif.de/anonyme-sim-karte-prepaid-discounter/news/52201.html (Accessed 8 August 2014.)

453 Vodafone. Law Enforcement Disclosure Report. op.cit. p. 65.

Government monitoring and centralization

At the time of writing India was considering implementing a Centralized Monitoring System, a surveillance scheme that would automate and centralize the process of interception and allow authorized security agencies to bypass ISPs to access and intercept communications directly.[454] Company privacy policies in context

Only some of the companies investigated in this case study publish privacy policies applicable to dedicated services offered locally (as opposed to website privacy policies, or general group-level policies published by the group headquarters as opposed to by the local subsidiary), or clearly and comprehensively explain what data they collect of users, how long they use it for, and what they do with it.

In Kenya, where there is no data protection legislation, ISPs were not found to have published comprehensive privacy policies for access by local users of their local services, and only briefly mentioned the possible instances of disclosure of user data in terms of service. Brazil also lacks a data protection or data retention law. According to the National Council of Justice,[455] in 2011 more than 18,000 telephone lines were monitored with judicial authorization. Besides telephone lines, 204 e-mail accounts and 673 lines using voice over IP were also monitored.

Also, despite legal mandates in many jurisdictions defining the time periods for which data must be retained, the companies studied do not specify in their terms of service or privacy policies (or at least those accessible to researchers) the exact time period for which they retain data.

Limitations on anonymous Internet use via both broadband and mobile data

In most of the countries investigated, legal requirements oblige users to sign up for services by presenting government-issued identification. This requirement typically applies to both post-pay and pre-paid services. These identification requirements are distinct from ISPs requiring personal information from the user for the carrying out of commercial transactions such as billing. Some jurisdictions legally obligate ISPs to verify this information before providing services to the user. This heavily reduces the space for anonymous online participation, as users' online behaviour may not only be tracked but also linked to their actual identity without the protections to privacy of international standards covering legitimate limitations of rights.

454 Human Rights Watch. India: New Monitoring System Threatens Rights. 7 June 2013. http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights (Accessed 26 June 2014.)

455 The National Council of Justice is a body composed by members of the Judiciary, the Public Prosecutor's Office, lawyers and members of civil society tasked with overseeing judicial malpractices and improving the management of the Judiciary.

3.4 Transparency

In a 2012 report "Opening the Lines: A call for transparency from Governments and Telecommunications companies" the Global Network Initiative recommends that ISPs and governments be transparent about the following: applicable laws and operating licenses, government requests for user metadata and content, government requests for filtering and government requests for text messages sent via the ISP's network without attribution.[456]

Transparency of laws, policies, practices, decisions, rationales, and outcomes related to privacy and restrictions on freedom of expression allow users to make informed choices about their own actions and speech online. Transparency is therefore important to internet users' ability to exercise their rights to privacy and freedom of expression.

3.4.1 Company Practices

The practice and scope of company and government transparency about surveillance practices, filtering and service restrictions vary across jurisdictions. In none of the countries studied are ISPs legally required to be transparent about their policy or practice regarding filtering, service restrictions, or surveillance measures. Below are some examples of ISPs' varying levels of transparency around specific types of restriction:

Commitment to notify users of restrictions based on government orders: None of the companies commit to provide individual or public notice of filtering based on orders from authorized authorities. Vodafone's 2014 Law Enforcement Disclosure Report does note that the company complies with filtering requests from authorized authorities.[457]

Commitment to notify users of restrictions based on self-regulatory steps: Almost all of the companies commit to notify the public of restrictions resulting from self-regulation. The exception is Vodafone UK, which notes in its Disclosure to Law Enforcement Report that the company filters child sexual abuse images on a wide and voluntary basis,[458] and notes in its terms of service that it will notify the customer of intention to suspend the service when reasonable. The Vodafone Group is also transparent about its collaboration with the IWF.[459] This could indicate that, beyond cooperation with self-regulatory bodies and internet hotlines, ISPs carry out few restrictions at their own initiative. In the Conditions of Use for PrePaid Services, Safaricom broadly states that the company will try to communicate with users through advertisement, newspaper, SMS, website or other suitable means.[460]

---

456 Tuppen. op. cit. p. 20
457 Vodafone. Law Enforcement Disclosure Report. op. cit. p. 68.
458 Vodafone. Child safety online – our approach. http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/child_safety_online.html
459 Vodafone. How to… report online child sexual abuse content to the IWF. http://www.vodafone.com/content/parents/howto-guides/internet_watch_foundation_helpline.html
460 Safaricom. Terms and Conditions PrePaid Mobile. section 8. http://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/conditions_of_use_for_the_safaricom_prepaid_services.pdf

Transparency about surveillance and user data requests: Other than Vodafone, none of the companies studied in this research publish information regarding the surveillance and user data requests that they receive and comply with. In January 2014, Vodafone challenged the UK government to permit it to disclose some information regarding governmental requests for wiretaps and user data.[461]

Neither Vivo nor its parent Telefonica, a Telecommunications Industry Dialogue member alongside Vodafone, has published data or general information about the nature and volume of government data requests or surveillance requirements. 'Transparency' is stated as an important value throughout Telefonica's 2013 Sustainability Report, but specifics are given only in relation to supply chain management and environmental sustainability.[462]

3.4.2 Implementation in national context

For ISPs and telecommunications services, the ability to be transparent with customers and users about practices affecting freedom of expression is heavily dependent on whether the government itself is transparent, and also whether legal frameworks allow meaningful levels of transparency on the part of companies.

Government transparency about restriction requests

In the jurisdictions covered by this case study, there is little government transparency about the nature and volume of official requests made to ISPs for filtering or service restrictions. Governments do not offer 'blacklist' overviews or official statistics about the number and type of restriction orders they issue. Sometimes governments acknowledge restrictions or respond to allegations of restriction in the media, or to queries from other branches of the government, although such instances are not standard or consistent. For example Egypt's National Telecommunication Regulatory Authority (NTRA) issued a press release in response to accusations in the media that it had ordered telecom companies to block or bar political words in their SMS services. In the press release the NTRA claimed this was untrue.[463] In India, news media reported in 2012 that in response to a question raised in Parliament, the Minister for Communication and IT noted that the Indian Government had asked social networking sites to block 1,299 URLs for various reasons including maintenance of public order.[464]

461 Juliette Garside. Vodafone takes a stand on privacy with plan to disclose wiretapping demands. The Guardian. http://www.theguardian.com/business/2014/jan/15/vodafone-aims-to-disclose-wiretap-demands (Accessed 13 July 2014.)

462 Telefonica 2013 Sustainability Report. op. cit.

463 NTRA Has Not & Will Never Interfere in the SMS Content. National Telecommunication Regulatory Authority. www.tra.gov.eg/english/News_NewsDetails.asp?ID=216

464 Government asks social networking sites to block 1,299 URLs. The Economic Times. 12 February 2014. http://articles.economictimes.indiatimes.com/2014-02-12/news/47270235_1_362-urls-62-urls-312-urls (Accessed 13 July 2014.)

Corporate transparency about restrictions in context

Some other intermediary types (such as Google, Facebook and Twitter examined in the next two case studies) offer 'transparency reports' with the number of content restriction requests received from governments and courts, the percentage complied with, and other data related to the company's handling of restrictions requested by authorized authorities. **In general, ISPs covered by this case research are not transparent about the extent to which they carry out filtering, their policies on filtering, or explanations about the legal requirements for filtering.**

Legal obstacles: One obstacle to greater transparency about filtering by ISPs is that in some jurisdictions ISPs are legally prohibited from publicizing filtering orders that they receive, as well as other information relating to content or service restrictions. For example, in India, ISPs are prohibited from disclosing details of governmental blocking orders by law,[465] while in the UK, ISPs are prohibited from publishing blocking orders relating to surveillance and terrorism, though not to copyright.[466]

General transparency: While Vodafone's Law Enforcement Disclosure Report recognized content and service restriction practices, it does not offer comprehensive information about scope of requests nor about the rate of compliance. Airtel India and Vodafone recognize in their terms of service that they comply with legal mandates for filtering, but few disclose all the actors – including government, law enforcement, commercial filtering companies and self-regulatory organizations – that are involved in filtering schemes and decisions. This makes it difficult to verify the legitimacy and justification of filtering actions.

Specific transparency: When a user tries to access a filtered website, some companies do display some form of explanation. For example, Airtel India and Vodafone UK display a notification screen when filtering takes place based on orders from authorized authorities or (in Vodafone's case) in accordance with co-regulatory mechanisms.[467] An example of a notice from Airtel India reads: 'This website/URL has been blocked until further notice either pursuant to Court orders or on the Directions issued by the Department of Telecommunications.'[468] Vodafone offers the following message for age-restricted mobile content:

---

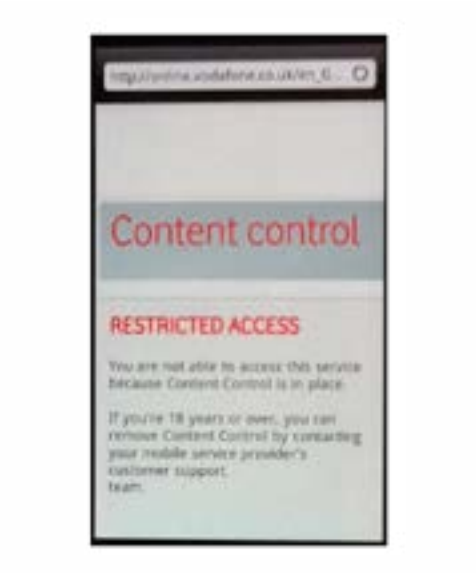
465 According to Rule 16 of the Information Technology (Procedures and Safeguards for Blocking for Access of Information by Public) Rules, 2009, blocking requests and complaints must be kept confidential. For more information see: http://dispur.nic.in/itact/it-procedure-safeguards-blocking-access-rules-2009.pdf.

466 See, inter alia, Regulation of Investigatory Powers Act 2000. s 97A Copyright Designs and Patents Act 1988, s3, Terrorism Act 2006, and s 21D Terrorism Act 2000.

467 See screenshot below.

468 For example, according to news items "Airtel users are shown a message "This website/URL has been blocked until further notice either pursuant to Court orders or on the Directions issued by the Department of Telecommunications". For more information see: http://www.medianama.com/2014/02/223-uploaded-net-blocked-again/.

Figure 2: Vodafone mobile 'restricted access' notice[469]



Government transparency about surveillance and user data requests

As noted in the Vodafone Disclosure to Law Enforcement Report, the German and UK governments provide official annual statistics about the number of interception and user data requests they issue. For example, in 2012, Germany requested Internet traffic data in 18,026 cases[470] and intercepted 23,687 telecommunications.[471] Similarly, the UK government authorized 2,760 interception warrants and 514,608 notices for communication data in 2013, according to the annual report of the Interception of Communications Commissioner.[472] Additionally, the audit conducted by the UK Commissioner found errors in the implementation of interception orders including: interception of incorrect communications addresses; interception and requests for stored communications made without lawful authority; inadequate discharge of legislative powers; failure to take steps to cancel erroneous interception; and telephone numbers attributed to the wrong target.[473]

469 Screentshot published by the Tor Project: https://blog.torproject.org/files/www.torproject.org-vodafone.png

470 Bundesamt für Justiz [Federal Office of Justice]. Übersicht Verkehrsdatenerhebung (Maßnahmen nach § 100g StPO) für 2012 [Summary of traffic data collection for 2012, first and extended orders] 1 August 2013. https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_Verkehrsdaten_2012.pdf

471 Bundesamt für Justiz [Federal Office of Justice]. Übersicht Telekommunikationsüberwachung (Maßnahmen nach §100a StPO) für 2012 [Summary of telecommunication surveillance for 2012, first and extended orders]. 24 October 2013. https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2012.pdf

472 Rt. Hon. Sir Anthony May. 2013 Annual Report of the Interception Communications Commisioner. p. 9. http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

473 Ibid. p. 16.

The other jurisdictions studied in this report have not published official information about surveillance and user data requests made to ISPs.

Corporate transparency about surveillance and user data in context

Legal constraints on what can be disclosed: Though the German government publishes statistics regarding interception and access to communications data, Vodafone stated confirmed in its Disclosure to Law Enforcement Report that it was not allowed to publish statistics about the lawful interception or user data requests received from German authorities. The report also explains that, given legal constraints, it would be difficult to explain a number of factors necessary to understand the meaning of these numbers. For example, such statistics would present only a partial view of law enforcement demands as they would not include automated access systems that allow rapid and large-scale interrogation of a central database of customer records.[474]

The revelations by former NSA contractor Edward Snowden pointed to apparent widespread data harvesting taking place by US and UK governments from a number of ISPs, including Vodafone UK. News reports in late 2013 claimed that some ISPs had gone well beyond what was required by law to assist intelligence agencies in their mass collection of communication.[475] Other reports associated Vodafone with this cooperation – codenamed 'Tempora' according to leaked documents.[476] Reports also asserted that Vodafone, among other companies, had given GCHQ unlimited access to its network of undersea cables.[477] Similar allegations have been made in the Egyptian media against Vodafone Egypt – accusing the company, along with other multinational ISPs operating in Egypt, of colluding with the Egyptian Government and allowing access to private communication data.[478] With regards to Egypt, Vodafone has denied these claims, and in its June 2014 Disclosure to Law Enforcement Report notes that the company may not disclose whether or not there are lawful intercept capabilities employed in Egypt.[479] With regards to the UK allegations, Vodafone also put out a statement in which it said that it did not recognize any of the UK intelligence agency programmes identified in the media, and that it never went beyond its legal obligations to collaborate with any security or intelligence agency by opening up its networks to any form of mass observation.[480] At its 2014 Annual General Meeting Vodafone also stated that the company would submit

474 Vodafone. Country-by-country disclosure of law enforcement assistance demands. Germany. June 2014. http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html

475 James Ball. Leaked memos reveal GCHQ efforts to keep mass surveillance secret. The Guardian. 25 October 2013. http://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden (Accessed 28 June 2014.)

476 James Ball, Luke Harding, and Juliette Garside. BT and Vodafone among telecoms companies passing details to GCHQ. 2 August 2013. http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq (Accessed 28 June 2014.)

477 Ibid.

478 Juliette Garside. Vodafone under fire for bowing to Egyptian pressure. 26 July 2011. http://www.theguardian.com/business/2011/jul/26/vodafone-access-egypt-shutdown (Accessed 28 June 2014.)

479 Vodafone. Country-by-country disclosure of law enforcement assistance demands. Egypt. op. cit.

480 Vodafone statement regarding GCHQ allegations. http://www.vodafone.com/content/index/media/faqs_statements/vodafone_statement.html

comments to a UK Government review of surveillance laws, and that its comments would be consistent with the principles outlined in its Law Enforcement Disclosure report.[481]

Lack of clarity about what is legal to disclose: At times, laws do not explicitly prohibit ISPs from disclosing information about surveillance and filtering, but when asked to clarify, authorities have made statements that conflict with existing practices. For example, although German law neither clearly prohibits nor allows ISPs to disclose such information, when Vodafone asked to confirm, authorities told it that publication would be against the law.[482] Yet a month before Vodafone published its report, German telecommunications provider Deutsche Telekom[483] and smaller email provider Posteo[484] had published transparency reports after having received permission from the government to publish 'anonymous statistical information'.[485] According to Vodafone, information published by other German telecommunication companies is incomplete and at risk of future prohibition.[486]

3.5 Remedy

For ISPs in jurisdictions covered by this research, potential remedy can potentially be provided for an individual user or an entire group of users whose right to freedom of expression has been infringed. Remedy can include an investigation, a public report/explanation, the reinstatement of content or connection, or can include the provisioning of an alternate means through which users are able to express themselves. These examples demonstrate that it is possible for courts or tribunals, companies, and regulatory bodies to grant remedy. The form of remedy available to users depends on the jurisdiction of the company and the user.

---

481 Peter Micek. Vodafone hears Access calls to go beyond transparency. 29 July 2014. https://www.accessnow.org/blog/2014/07/29/vodafone-hears-access-calls-to-go-beyond-transparency (Accessed 13 August, 2014.)

482 Vodafone. Country-by-country disclosure of law enforcement assistance demands. Germany. op. cit.

483 Deutsche Telekom. Jahresbericht – Auskunft an Sicherheitsbehörden. [Annual report – Information to security agencies]. (In German.) 5 May 2014. www.telekom.com/sicherheitsbehoerden (Accessed 13 August 2014) and Kirsten Gollatz. 20 May 2014. Deutsche Telekom's 'surveillance report' builds on a trend. Internet Policy Review. http://policyreview.info/articles/news/deutsche-telekoms-surveillance-report-builds-trend/284 (Accessed 13 August 2014.)

484 Posteo. 5 May 2014. Transparenzbericht. [Transparency report]. (In German.) https://posteo.de/site/transparenzbericht_2013 (Accessed 13 August 2014.)

485 Transparenzbericht. Posteo. 5 May 2014, https://posteo.de/site/transparenzbericht_2013 (Accessed 28 June 2014); Deutsche Telekom. Provision of information to security authorities. 12 June 2014. http://www.telekom.com/corporate-responsibility/data-protection/More+Articles/239498; and Posteo. Ihre schriftliche Frage Nr. 4/175 vom 17. April 2014. 29 April 2014, https://posteo.de/Antwort_Bundesregierung.pdf

486 Vodafone. Country-by-country disclosure of law enforcement assistance demands. Germany. op. cit.

3.5.1 Company Dispute Resolution Mechanisms

Mechanisms for complaints and dispute resolution can potentially complement, or serve as an alternative to, systems for redress and remedy provided by government. Some governments require that companies institute private grievance and remedy mechanisms.

Options limited to consumer complaints

Airtel India provides a mechanism for the resolution of differences arising between subscribers and the company. The arbitrator of these disputes will be appointed by Airtel India and the resolution of the dispute will be subject to the jurisdiction of the city where installation is opted for.[487] As required by the law[488], Airtel India additionally lists the contact information of a grievance officer in their online privacy policy,[489] as well as the contact information of regional Appellate Authorities that individuals can contact if their complaints are not resolved at the nodal officer level.[490]

Vodafone UK has a number of potential paths that users can follow to lodge complaints. For example, it is suggested that users initially submit complaints to the 'account manager' via the 'customer complaint code,' which offers a live helpline. Complaints are handled by customer care, but if not resolved within eight weeks, can be escalated to an independent ombudsman.[491] Vodafone UK also outlines an 'escalation route' that customers are expected to exhaust before bringing legal action. Additionally, it is clarified that both parties are subject to the UK Data Protection Act 1998, under which Vodafone is a data controller. This is potentially a strong mechanism through which users can seek redress for breaches regarding their data.[492] The General Terms and Conditions also specify an address for the sending of notices, and note that in the situation where Vodafone will suspend end users from use of the service, Vodafone will first inform the customer to allow for potential remedy of the alleged breach.[493] Lastly, Vodafone UK clarifies that if there is a misrepresentation or untrue statement, the only remedy available to customers is through a claim for damages for breach of contract.[494]

The UK also has a co-regulatory mechanism for remedy: In a 2014 Ofcom Report on the family friendly network level filtering services that the major fixed-line ISPs are offering the

---

487 Airtel India. Terms and Conditions. section 18. op. cit.

488 According to Rule 5(9) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, all body corporate handling sensitive personal information in the digital format must list the contact information of a grievance officer on their website. http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

489 Airtel India. Privacy Policy: Feedback and Concerns. http://www.airtel.in/forme/privacy-policy/feedbak?contentIDR=c9d0f414-8cb9-4381-b122-3f3148a01b80&useDefaultText=0&useDefaultDesc=0

490 Airtel India. Broadband Internet Appellate Authorities. http://www.airtel.in/applications/xm/BroadbandInternet_AppellateAuth.jsp

491 Vodafone UK. Contact Us. http://www.vodafone.co.uk/contact-us/

492 Vodafone. General Terms. provision 17.2 http://www.vodafone.co.uk/about-this-site/terms-and-conditions/general-terms/

493 Vodafone. General Terms. provision 3 and 17.3. http://www.vodafone.co.uk/about-this-site/terms-and-conditions/general-terms/

494 Vodafone. General Terms. provision 17.8. http://www.vodafone.co.uk/about-this-site/terms-and-conditions/general-terms/

UK, it is noted that customers and site owners can follow a process to report websites or content that have been incorrectly filtered – leading to a review of the categorization of identified content for filtering.[495]

Safaricom does not provide as much detail as Vodafone UK, but does note in the Term and Conditions for prepaid mobile services, that all disputes must be settled by a single arbitrator that is agreed and appointed by both parties. Any award must be made under the Arbitration Act 1995 and all disputes are subject to the jurisdiction of Kenya. All determinations by the Arbitrator will be final and binding.[496] Airtel Kenya does not mention a dispute resolution mechanism in their terms of service and does not appear to have a complaint mechanism on their website.

While filtering is not relevant for Vivo in Brazil, it is possible that users may have grievances related to privacy violations. While there is no publicly available information about remedy or grievance mechanisms offered by Vivo, Telefonica's 2013 Sustainability Report states that the Group has committed to 'examine, as a group, options for implementing relevant grievance mechanisms, as outlined in Principle 31 of the UN Guiding Principles for Business and Human Rights', and that Telefonica is exploring 'this aspect' as a member of the Telecommunications Industry Dialogue.[497]

Complaint mechanisms offered by industry organizations and regulators

The UK Internet Service Providers' Association (ISPA) offers a complaints mechanism through which users can issue complaints against companies that are members of ISPA for violation of the ISPA code of conduct.[498] Additionally, the UK telecommunications regulator Ofcom offers a complaint mechanism for users which includes avenues for issuing complaints related to the safety of the user's personal information, the recording of phone calls, and content that is believed to be illegal – in which users are directed to report content that is thought to be illegal to the Internet Watch Foundation.[499] Types of content that are listed as examples of illegal content include: images of child sexual abuse, criminally obscene adult material that is hosted in the UK, and incitement to racial hatred that is hosted in the UK.[500]

Similarly, the Telecom Regulatory Authority of India (TRAI) has developed the 'Telecom Consumer Complaint Redressal Regulations, 2012' that governs how ISPs must structure consumer complaint mechanisms at the organizational level and how complaints should be responded to (time frames etc). Complaints, including those 'alleging that a practice

---

495 Ofcom Report on Internet safety measures. Internet Service Providers: Network level filtering measures. 22 July 2014. http://stakeholders.ofcom.org.uk/binaries/internet/internet_safety_measures_2.pdf

496 Safaricom. Conditions of Use for the Safaricom Prepaid Services. http://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/conditions_of_use_for_the_safaricom_prepaid_services.pdf

497 Telefonica 2013 Sustainability Report, op. cit p. 129

498 The Internet Service Providers Association. Complaints Form. http://www.ispa.org.uk/consumers/complaints-form/

499 Other issues: Scams and frauds. Ofcom. http://consumers.ofcom.org.uk/complain/phone-and-broadband-complaints/other-issues/

500 Ibid.

adopted by the service provider adversely affects the interest of the consumers' can also be issued to TRAI and referred by TRAI to the relevant ISP.[501] TRAI also accepts responses from companies to present and proposed policies impacting their services. In a move towards protecting user privacy and freedom of expression, Airtel India in 2012 submitted a response to regulations meant to govern and control unsolicited commercial communications. In the response, Airtel stressed the need for privacy legislation in India and argued against using any 'artificial intelligence criterion' for blocking text messages (such as imposing a numeric limit per user per hour) because it 'would amount to interfering with the cherished right of freedom of speech and expression.'[502]

3.5.2 Role of the Legal System and Consumer Protection Bodies

Obtaining remedy through the courts can be time-consuming and expensive in many countries. Little international research has been done in relation to best practices for consumer protection bodies in handling cases related to telecommunications. Nonetheless, researchers found two particularly notable examples of remedy: one through the courts and the other through consumer protection bodies.

Accountability through courts: In May 2011 an Egyptian Court issued a fine of $90 million to the former President Hosni Mubarak and Vodafone, Mobinil and Etisalat. The ruling held that the president, the prime minister and interior minister were responsible for damages to the economy while the ISPs had violated the Egyptian Constitution for complying with a request that was not accompanied with a legally issued warrant.[503]

Consumer protection mechanisms: In 2012 Airtel India was ordered by a consumer forum to pay a user rs.15,000 (approximately USD 300) for 'harassing' a customer and for disconnecting the call services to the user's phone for 24 days.[504] Also in 2012, Airtel India was fined by a Karnataka consumer forum Rs.20,000 (approximately USD 400) for 'deficiency in Internet service' and causing mental agony to the complainant by incorrectly blocking websites and subsequently being unable to download an application.[505]

---

501 Telecom Consumers Complaint Redressal Regulations, 2012. Telecom Regulatory Authority of India. 5 January 2012. http://www.dot.gov.in/sites/default/files/TCCRR0012012.pdf

502 Bharti Airtel's response to TRAI Consultation paper (No. 13/2012) on Review of The Telecom Commercial Communications Customer Preference Regulation, 2010 and The draft Telecom Commercial Communications Customer Preference (Tenth Amendment) Regulation, 2012. http://www.trai.gov.in/WriteReadData/ConsultationPaper/Document/20120905052555337402 36.%20Airtel%20response.pdf

503 Egypt: Court fines Mubarak and Vodafone for communications blackouts. Association for Progressive Communications. 30 May 2011. http://www.apc.org/en/press/egypt-court-fines-mubarak-and-vodafone-communicati (Accessed 18 July 2014.)

504 Airtel fined Rs. 15,000 for 'harassing' customer. Times of India. 31 August 2012. http://timesofindia.indiatimes.com/tech/tech-news/Airtel-fined-Rs-15000-for-harassing-customer/articleshow/16060415.cms (Accessed 14 July 2014.)

505 Anuj Srivas. Airtel penalised for 'torrent site' block, legality questioned. 7 August 2012. http://www.thehindu.com/sci-tech/technology/internet/article3738269.ece (Accessed 14 July 2014.)

3.6 Conclusions

Across jurisdictions, stakeholders interviewed for this research highlighted the importance of ISPs and the fundamental role that they play in connecting users to a wealth of knowledge, opportunities, and possibilities for expression. Yet some users feel that companies need to do more to protect freedom of expression.

For example, users in Egypt, particularly with respect to Vodafone's cooperation with the Egyptian Government, have expressed the view that ISPs need to do more to resist governmental demands for user data.[506] Safaricom in 2014 was the target of public and media criticism for violating users' privacy by sending out SMS messages on behalf of the National Council of Churches of Kenya.[507] Civil society groups such as the US-based Access have also criticized the company for sharing user data without consent. Access has called on the company to conduct a thorough human rights impact assessment and reform its policies affecting privacy and freedom of expression.[508] Companies such as Vodafone have pointed out that defying government requests can pose high risk for ISPs – business risks as well as risks to the safety of their local employees. On the other hand, through compliance in some cases, companies may also risk damaging the trust of their users.

A number of general observations can be drawn from this case study's findings:

Governments and companies offer even less transparency about restrictions of expression made by and through ISPs than about policies and practices related to privacy and surveillance. The findings of this case study highlight a severe lack of transparency by governments and companies across a range of jurisdictions about basic aspects of filtering practices. In the wake of the revelations from Edward Snowden, public dialogues and research initiatives have been heavily focused on the obligation of ISPs and governments to be transparent about privacy and surveillance requests, with much less emphasis on transparency of practices that directly affect internet users' freedom of expresison.[509]

---

506 Political activists attack Vodafone Egypt on Twitter. The Cairo Post. 4 January 2014. http://thecairopost.com/news/66987/quirk_of_the_day/political-activists-attack-vodafone-egypt-on-twitter (Accessed 10 August 2014.)

507 Njeri Wangari. CCK approved SMS Message from NCCK causes a storm with Kenyans Online. Afromum. 4 July 2014. http://www.afromum.com/cck-approved-sms-message-from-ncck-causes-a-storm-with-kenyans-online/ (Accessed 10 August 2014.)

508 Ephraim Percy Kenyanito. Surveillance in a legal vacuum: Kenya considers massive new spying system. Access blog. 13 June 2014. https://www.accessnow.org/blog/2014/06/13/surveillance-in-a-legal-vacuum-kenya-considers-massive-new-spying-system (Accessed 10 August 2014.)

509 For example, Some projects testing ISP transparency, such as IXmaps, have developed criteria broadly related to the public commitment to applicable data protection law, public commitment to inform users about third party requests for information, transparency about frequency of third party requests, inclusive definitions of personal information, retention periods for personal information, transparency about where personal information is stored, transparency about where personal information is routed, visible steps to avoid U.S routing of data, and open advocacy of user privacy rights. For more information see: http://ixmaps.ca/transparency.php

On surveillance, government transparency is limited and few companies speak up for their users. The German and UK governments publish annual reports reviewing the scope of government surveillance. Vodafone publishes clear policy guidelines on how it deals with government requests for user data. Though this is a positive, it leaves subscribers of the other services in the dark about how their privacy will be protected in the face of government or other pressures. This uncertainty is compounded by the lack of information on government user data requests. As of this report's writing, Vodafone was the only company to report on the number of user data requests it receives from government agencies. The numbers of users whose information is requested is significant, even though no numbers about compliance are provided. Although Safaricom was included in the Law Enforcement Disclosure Report, Vodafone was unable to disclose the number of government requests because it was unable to determine whether disclosure would be lawful.[510]

It is notable that Vodafone is also the only company covered in this research calling openly for greater government transparency, and for legal reforms that would enable the company itself to report more detail about surveillance and user data requests.

Data protection and privacy practices of companies vary widely, in tandem with the existence or lack of data protection laws. As described in section 2.1.2, with the exception of the EU's data protection framework, data protection regimes in other countries studied are in a state of flux: Kenya and Brazil have data protection bills under varying stages of parliamentary consideration and India at the time of writing has no comprehensive data protection law. Research for this study showed a clear connection between weaker privacy laws and weaker privacy policies by ISPs. ISPs in countries with weaker or nascent legislation also disclosed much less information about their privacy-related practices. Such findings underscore the need for comprehensive data protection laws at the national level.

It is difficult for individuals, as users and citizens, to hold companies and governments accountable for actions taken via ISPs that restrict users' freedom of expression in a manner incompatible with international human rights standards. In some jurisdictions, industry regulators can offer means by which users can report infringing content or report ISP practices that violate their rights. In some jurisdictions, such as India, it appears that users can hold ISPs accountable through consumer tribunals. However examples from this research of redress for violations by ISPs and or government agencies of users' online freedom of expression have been limited to monetary fines. This shows that recognition and consequence for violations is limited.

Public commitments by some companies to international human rights principles are an important first step but there is a long way to go. In March 2013, a group of telecommunications operators and vendors including internet service providers launched the Telecommunications Industry Dialogue on Freedom of Expression and Privacy

510 Vodafone Law Enforcement Disclosure Report, op. cit. p. 78.

(hereafter 'Industry Dialogue') with a set of 'Guiding Principles' influenced by the UN Guiding Principles on Business and Human Rights.[511] Vodafone and Telefonica at the time of writing were among the 9 Industry Dialogue members, and their 2014 reports cited in this case study are billed on the ID website as a product of the companies' commitment to report annually on 'progress in implementing the principles and, as appropriate, on major events occurring in this regard.'[512]

As discussed earlier in this case study, the Vodafone and Telefonica reports vary greatly in the extent to which they offer specifics about company policies and practices. For example, the privacy-related practices of Telefonica's subsidiary, Vivo, remain particularly opaque. Nonetheless, it is notable that these two Industry Dialogue members have made clear public commitments to respect user rights and to examine group-wide policies and practices in light of those commitments. The two non-Industry Dialogue members studied in this research, Bharti Airtel and Safaricom, have made no similar public commitments.[513]

The Industry Dialogue is engaging in collective study of best practices in corporate transparency for their sector, as well as 'how to implement operational-level grievance mechanisms'. Members have also acted collectively to engage with governments. As their first annual report states, the Industry Dialogue's intention to 'continue to advocate for greater government transparency on the use and scope of surveillance of communications and on actions that have the effect of restricting the content of communications, in keeping with our Principles.'[514]

The concrete impact of such company activities and commitments on internet users has yet to be studied systematically, let alone measured. Nonetheless, activities of the Industry Dialogue member companies thus far indicate that collective action, combined with broader stakeholder engagement, has empowered ISPs to take steps that they had previously not been willing to take on their own. Thus it seems that users in countries where Bharti Airtel and Safaricom operate would only stand to benefit in the long run if those two companies should ever join the Industry Dialogue as active and committed members. The Industry Dialogue would benefit further in terms of credibility by adding an assurance process to verify whether companies are implementing their commitments, overseen by a multistakeholder board, such as the third-party assessments carried out by the Global Network Initiative.

511 Telecommunications Industry Dialogue 'About' page. http://www.telecomindustrydialogue.org/about

512 Telecommunications Industry Dialogue. Guiding Principles. http://www.telecomindustrydialogue.org/content/guiding-principles

513 Although Vodafone implies with its inclusion of Safaricom in its 'Disclosure to Law Enforcement' report that even with only 40% ownership it asserts some level of influence on Safaricom's policies and practices.

514 Telecommunications Industry Dialogue. Annual Report 2014. http://www.telecomindustrydialogue.org/sites/default/files/ID%20Annual%20Report%202014.pdf

4. STUDY 2: SEARCH ENGINES

Google (USA, EU, India, China, Russia), Baidu (China), Yandex (Russia)

4.1 Introduction

Search engines are a principal means by which Internet users find and access information. They are important for freedom of expression because they act as an intermediary between people who seek information and people who publish information on the Web in hopes of reaching larger audiences. As one journalist has described: they are a "shaper of online reality, helping determine what we see and how."[515]

Most web pages on the internet are not indexed by search engines and therefore cannot be found in search engine results.[516] Even Google, the world's largest and most popular search engine, has only indexed a small percentage of the world's web pages (estimates range from 0.4 to 12 per cent).[517] There are three main reasons for this: a) the web pages have not yet been found or cannot be found by the spiders because no other websites link to them; b) they are "invisible" to spiders because the owners of web pages and online databases have chosen to block them; c) the database structure of most websites "hides" pages from discovery by an external spider.[518]

Every search engine uses its own search algorithm, a complex mathematical formula that decides what results to display, and in what order, in response to a user's specific query.[519] The algorithm's decisions about what is most relevant to the searcher are triggered in part by elements in a web page's URL, headlines on the page, and other content in the page itself. Those who want their content to be viewed by large audiences of search engine users can "optimize" their Web sites, pages and content not only so that it will be found and indexed, but also to maximize the probability that it will appear near the top of the first page of a search engine's displayed results.[520]

---

515 Craig Timberg. 12 May 2014. Research in India Suggests Google Search Results Can Influence an Election. *Washington Post*. The Switch blog. www.washingtonpost.com/blogs/the-switch/wp/2014/05/12/research-in-india-suggests-google-search-results-can-influence-an-election. (Accessed 19 April 2014.)

516 Michael K. Bergman. August, 2001. White Paper: The Deep Web: Surfacing Hidden Value. *Taking License*. Vol 7 Issue 1. http://quod.lib.umich.edu/j/jep/3336451.0007.104 (Accessed 19 April 2014.)

517 Brian Proffitt. 17 June 2013. Google Is Starting War On Child Pornography, Not Ending. *ReadWriteWeb.* http://readwrite.com/2013/06/17/google-is-beginning-war-on-child-pornography-not-ending#awesm=~oBTRHlVjKDVc11 (Accessed 14 July 2014.)

518 UC Berkeley Library. Invisible or Deep Web: What it is, How to find it, and Its inherent ambiguity. http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html (Accessed 19 April 2014.)

519 See Google. Inside Search: How Search Works: Algorithms. https://www.google.com/insidesearch/howsearchworks/algorithms.html

520 Search Engine Optimization. Microsoft Developer Network. http://msdn.microsoft.com/en-us/library/ff724016(v=expression.40).aspx

No two search engines will produce the same results—or the same number of results—for the same query, unless their algorithms, spiders, and indexes are identical. This is why, for example, if one searches for the same term on Google.com and Microsoft's Bing.com, on the same computer in the same location at the same time, the results will not be the same even if no deliberate effort has been made to restrict or manipulate results.

Freedom of expression in relation to search engines involves three potential parties: 1) individual internet users seeking information; 2) creators and operators of websites that are or potentially may be indexed by search engines; 3) the search engines themselves whose algorithms have been viewed by scholars and emerging jurisprudence as a kind of editorial process – albeit not as direct and deliberate as a media organization's editorial process.[521] This study examines how search engine policies and practices related to content restriction and content manipulation are shaped by their home jurisdictions, and to varying degrees by the laws and regulations of other jurisdictions. It also analyzes how three different companies headquartered in three very different national contexts have chosen to handle challenges related to online freedom of expression.

The companies

This case study focuses on three search engines, all run by companies that provide many other services beyond search:

Baidu dominates in China with 63.1 per cent market share of the world's largest Internet user base of over 600 million.[522]

Yandex dominates in Russia with 62 per cent market share in a country of 84.4 million Internet users.[523]

Google is the world's dominant search engine. Its market share in the United States (with 279.8 million Internet users[524]) is 67.5 per cent.[525] Google's market share is much higher in countries where there is no major local competitor. For example Google's market shares

521 Joris van Hoboken. *Search Engine Freedom: On the implications of the right to freedom of expression for the legal governance of Web search engines.* PhD thesis, University of Amsterdam Faculty of Law, 2012. *http://dare.uva.nl/document/357527* p.322

522 As of December 2013. Steven Millward. Baidu down, Qihoo up, Google dead: 2013 was a year of drama for China's search engines. *Tech In Asia*. 7 January 2014. www.techinasia.com/how-baidu-qihoo-google-performed-in-china-in-2013. (Accessed 21 May 2014.) However, Baidu itself claims a 70% market share. Baidu Introduction. http://is.baidu.com

523 As of April 2014, according to LiveInternet. See Smita Nair. Yandex sees a market share increase powered by its search service. Yahoo Finance. 31 March 2014. http://finance.yahoo.com/news/yandex-sees-market-share-increase-130033283.html (Accessed 21 May 2014).

524 Internet Live Stats http://www.internetlivestats.com/internet-users-by-country/ (Accessed 7 August 2014.)

525 Craig Smith. By The Numbers: 40 Amazing Google Stats and Facts. Digital Marketing Ramblings. http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts. (Accessed 21 May 2014.)

in India and European markets are 97 per cent and 90 per cent respectively.[526] Google's market share in Russia is 27.6 per cent[527] and a mere 1.6 per cent in China.[528]

China, **Russia**, the **United States** and **India** were chosen as focus countries where our researchers examined outcomes resulting from the interplay of company policy and practice with national legal contexts. The first three were chosen because they are the home markets of the three search engines. While China, Russia, and the US were chosen as they are the home markets of the three search engines, India was selected as it is a large developing nation and important market for global Internet companies, the common thread running through all three case studies. Where useful for the purposes of comparative analysis, outcomes in the **European Union** are also discussed.

4.2 Impact of Network Filtering on Search Engines

The freedom of expression of search engine users can be affected when a search engine is filtered by ISPs. If the search engine's front page is filtered, then the service is wholly inaccessible to users accessing the Internet via that particular ISP or national network. It is also possible for the ISP to filter only specific pages of search engine results containing specific URLs or keywords, making the service partially usable – as long as the user is not searching for content that is filtered by the ISP.

The search engine operator has no control over—and plays no role in—filtering by ISPs. However, the nature and extent of ISP filtering in a given jurisdiction affects how search engines in turn carry out their own restrictions. Thus, prior to a discussion of the policies, practices, and implementation of restrictions by the three search engines themselves, it is necessary to describe the extent and nature of ISP filtering of search engines in each country covered in this case study. In the four jurisdictions covered by this case study, four different approaches to search engine filtering were identified:

No filtering of search engines:

In the United States, ISPs do not filter search engines at any level, although targeted filtering based on keywords or URLs occurs at the level of the home or institution level (schools, libraries, hotels, corporations, specific government agencies, etc.).[529] Any broader restriction of search engine results is implemented by the search engine itself (as will be described in section 4.3).

---

526 Paul Geitner. Google Moves Toward Settlement of European Antitrust Investigation. *New York Times*. 25 July 2012, www.nytimes.com/2012/07/25/technology/eu-nears-settlement-of-google-antitrust-investigation.html and Rohin Dharmakumar. Is Google Gobbling Up the Indian Internet Space? *Forbes India*. 22 July 2013. http://forbesindia.com/article/real-issue/is-google-gobbling-up-the-indian-internet-space/35641/0 (Accessed 21 May 2014.)

527 As of April 2014. LiveInternet. www.liveinternet.ru/stat/ru/searches.html?slice=ru;period=month.

528 As of December 2013. Steven Millward, op. cit.

529 John G. Palfrey, Jr. Local Nets on a Global Network: Filtering and the Internet Governance Problem. THE GLOBAL FLOW OF INFORMATION, Jack Balkin, ed. Harvard Public Law Working Paper Nº 10-41. p.8. Available at SSRN: http://ssrn.com/abstract=1655006.

Filtering of websites but not the search engines:

In Russia, since 2012 ISP's are required to filter blacklisted websites.[530] Thus if a user of Google or Yandex conducts a search whose results include a link to a blacklisted website, and if he or she clicks on that link, an error message will be displayed in place of the website. The message, generated by the ISP, explains that the page has been filtered in compliance with law. Below is an example of such a page in Russian. In English translation it reads:

Dear users!

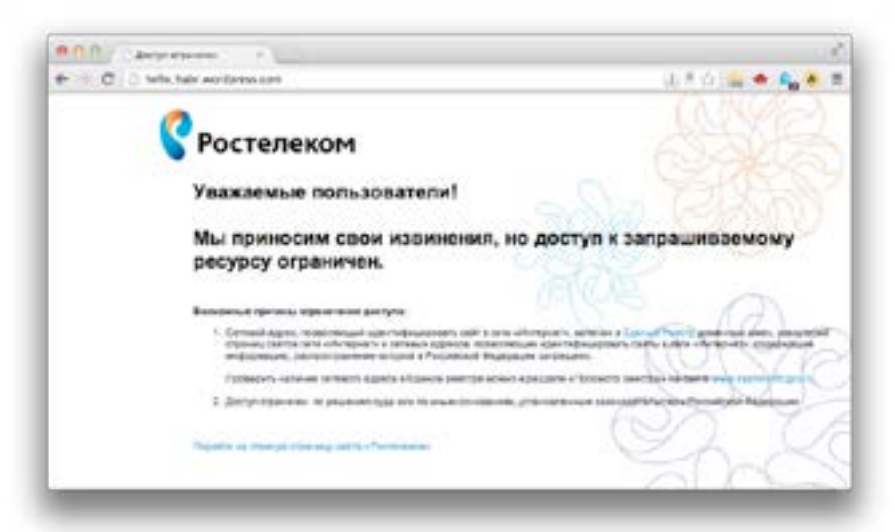
We beg your pardon, but access to the requested services is now limited.

Possible reasons for it:

1. The network address identifying the web site on the internet is included in the 'General list of domain names that include prohibited information.'

2. The access is limited in accordance with a court decision or other Russian legal norms.

Figure 3: Error message displayed for filtered website in Russia



Limited filtering of search engines:

In India, Google (or other search engines) are generally not filtered through governmental orders. An exception to this is the temporary 'internet blackout' ordered by the

530 J.Y. Lurk no more: Internet censorship in Russia. *The Economist* Eastern approaches blog. http://www.economist.com/blogs/easternapproaches/2012/11/internet-censorship-russia (Accessed 21 May 2014.)

Government of Jammu and Kashmir in 2012 in response to violent outbreaks after the release of the 'innocence of Muslims' YouTube film,[531] during which all search engines and other websites were rendered inaccessible. Additionally, in 2012 the Delhi High Court threatened to block Google and other internet services if they did not take steps to monitor and remove objectionable content from their platforms.[532]

Extensive filtering of overseas search engines accompanied by temporary disconnection from the internet:

The phenomenon of internet filtering in China has been the subject of extensive research and scholarly publication over the past decade.[533] While it is beyond the scope of this case study to provide an in-depth summary of that research, it is nonetheless important to understand some basic characteristics of Internet filtering in China in order to understand how filtering affects freedom of expression for Chinese search engine users – and for websites aiming to reach audiences in China.

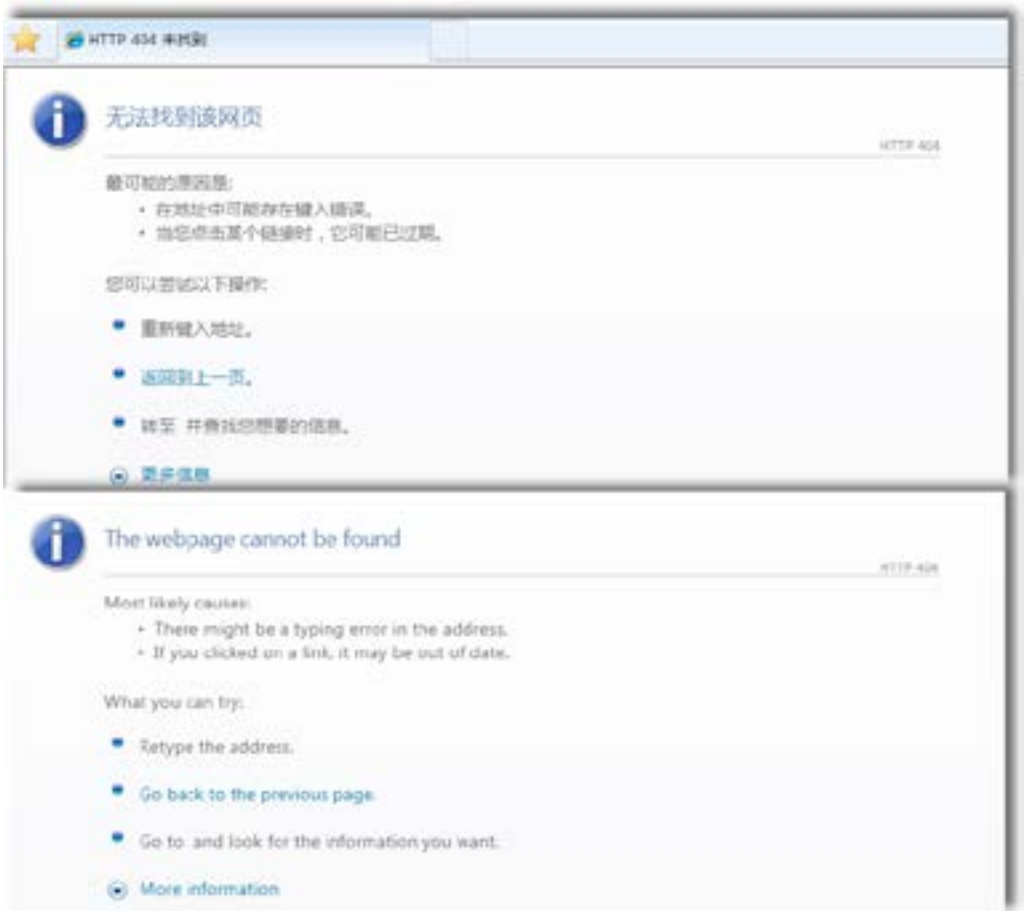
In China blacklisted websites are filtered, as are web pages containing politically sensitive words or banned URLs, including pages displaying search queries and search results containing sensitive words. When a user tries to access a filtered URL, or a page containing filtered keywords or links, an error message stating "the webpage cannot be found" appears in his or her browser. Below is how the message appears in an Internet Explorer browser:

531 J&K govt orders blackout of anti-Islam film, blocks internet. Indiatoday. 21 September 2012. http://indiatoday.intoday.in/story/jammu-and-kashmir-govt-orders-blackout-of-anti-islam-film-blocks-internet/1/221569.html (Accessed: 16 April 2014.)

532 Filter content or face blackout, Delhi HC warns Facebook, Google. Reddiff.com. 13 January 2012. http://www.rediff.com/money/slide-show/slide-show-1-tech-delhi-hc-warns-facebook-google/20120113.htm (Accessed: 16 April 2014.)

533 See for example Jonathan Zittrain and Ben Edelman. Internet Filtering in China. IEEE Internet Computing March/April 2003. http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan011043.pdf; OpenNet Initiative. Internet Filtering in China in 2004-2005: A Country Study. https://opennet.net/studies/china; and Xueyang Xu, Z. Morley Mao, and J. Alex Halderman. Internet Censorship in China:
Where Does the Filtering Occur? In Proceedings of PAM . 2011. http://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf.

Figure 4: "This website cannot be found" browser error in China.



No notification or explanation of the restriction is provided to the user from the ISP or other authorities. However – assuming that the user indeed made no errors in typing the URL and the link is not out of date as the error message implies – technical testing confirms that the appearance of this error message indicates that the webpage has in fact been filtered. At the same time that the browser displays this error message the user's internet connection is disconnected for anywhere between several seconds to a few minutes. [534]

All web content and services including search engines operating from outside China's jurisdiction are filtered when their content passes through internet exchange points via which all internet traffic is routed in and out of the country – with the exception of Hong

534 Xu, Mao, and Halderman. op. cit. p. 137 and James Fallows. 'The Connection Has Been Reset'. *The Atlantic*. 1 March 2008. http://www.theatlantic.com/magazine/archive/2008/03/-the-connection-has-been-reset/306650/ (Accessed 22 May 2014.)

Kong.[535] If the entire search engine is blacklisted, then the entire service is inaccessible. If only specific keywords and URLs are programmed into the filtering blacklist, then the front page of the search engine is accessible but searches on certain terms will trigger the filters, resulting in the error page pictured above as well as a temporary disconnection of internet service. Such disruption makes search engines operating from outside very inconvenient to use in China even when their main search page is accessible.

Within China, ISP level filters are not as extensive as the filters deployed at the exchange points controlling international traffic.[536] Websites operating from within the jurisdiction of China are not subject to the same degree of filtering because they carry out their own content restrictions in response to government requests and requirements (see section 4.3 of this study and Study 3 for more detail).

4.3 Measures Taken by Search Engines

In any given jurisdiction, search engine operators may restrict or manipulate content through any or all of the following actions:

1. remove specific pages or even entire websites from the search engine's index;
2. program the spider not to add certain pages, entire websites, or sites containing certain content;
3. program the search engine's algorithm not to deliver results for certain queries;
4. program the algorithm to favour or "weight" certain types of web pages over others;
5. influence the user's understanding of certain search results by adding explanatory statements, warnings, or statements in accompanying advertising.

As with the service providers discussed in the previous case study, search engines may restrict content at the request of a government authority or other external party, or may restrict content to enforce their own terms of service and other private rules or procedures.

Personalization: In 2005 Google started tailoring search results for all logged-in users to their apparent preferences and interests based on search history. In 2009 personalization was extended to all Google searches even if the user is logged out, based on browser cookie records.[537] Critics have expressed concern about the effect of personalization on freedom of expression because it renders the same website more or less visible to different

535 Xu, Mao, and Halderman, op. cit. pp. 133-142; also see James T. Areddy. Birds Above, Data Below: Where the U.S. Internet Meets China's. *The Wall Street Journal* China Realtime blog. 8 July 2014. http://blogs.wsj.com/chinarealtime/2014/07/08/birds-above-data-below-where-the-u-s-internet-meets-chinas/ and James T. Areddy, Paul Mozur, and Danny Yadron. From Mountains, Island, Secret Town, China's Electronic Spy Shop Watches. *The Wall Street Journal.* 7 July 2014. http://online.wsj.com/articles/chinas-spy-agency-has-broad-reach-1404781324. (Accessed 10 August 2014.)

536 Xu, Mao , and Halderman, op. cit.

537 Personalized Search for Everyone. Google Official Blog. 4 December 2009. http://googleblog.blogspot.com/2009/12/personalized-search-for-everyone.html (Accessed 14 September, 2014.)

users depending on their prior browsing habits.[538] The full impact of personalization on freedom of expression globally remains unclear. Some have argued that the issue is less about the degree of personalization and more about the extent to which the user is able to understand and control the factors affecting their own searches.[539] One recent academic study of Google searches found that personalization varies widely depending on the query, and that personalization was much less measurable for queries made on Google when logged out.[540] Personalization also occurs on Baidu and Yandex.[541]

4.3.1 Company policies on government requests and legal requirements

The legal environments of the companies' home jurisdictions heavily shape their policies and practices related to content restriction.

Baidu: Content forbidden by the terms of service overlaps directly with content designated as illegal in China. Specifically, as mentioned in Chapter 2, Article 15 of *Measures on the Administration of Internet Information Services*, (hereafter referred to as "Measures") stipulates what have come to be known as the "nine forbidden content categories" for Chinese online services.[542]

Under China's strict liability regime described in Chapter 2, all online services including search engines are held liable for failing to prevent content that falls into these "forbidden nine categories" from appearing on their platforms. Industry representatives interviewed for this report confirm that companies including Baidu receive regular instructions as well

538 Jessica Thompson. Search Personalization: Good or Bad? Advance Digital Search & Social Group. http://www.advancessg.com/search-personalization-good-or-bad/ (Accessed 14 September 2014.)

539 Van Hoboken, op. cit. p. 205

540 Aniko Hannak, Balachander Krishnamurthy, David Lazer, Christo Wilson, Arash Molavi Kakhki and Alan Mislove. Measuring Personalization of Web Search. WWW '13 Proceedings of the 22nd international conference on World Wide Web. pp. 527-538. http://www.ccs.neu.edu/home/cbw/pdf/fp039-hannak.pdf

541 Matt McGee. Yandex Turns Up The Dial On Personalized Search. Search Engine Land. 13 May 2013. http://searchengineland.com/yandex-turns-up-the-dial-on-personalized-search-161695 (Accessed 15 September, 2014) and Min Jiang. The Business and Politics of Search Engines: A Comparative Study of Baidu and Google's Search Results of Internet Events in China. http://www.researchgate.net/publication/256016569_The_Business_and_Politics_of_Search_Engines_A_Comparative_Study_of_Baidu_and_Googles_Search_Results_of_Internet_Events_in_China. *New Media & Society.* 16(2). pp. 212-233.

542 *Measures on the Administration of Internet Information Services*, http://www.net.cn/static/hosting/fa_xinxi.htm. The "nine forbidden categories" apply to content that: 1. Opposes the fundamental principles determined in the Constitution; 2. Compromises State security, discloses State secrets, subverts State power or damages national unity; 3.Harms the dignity or interests of the State; 4.Incites ethnic hatred or racial discrimination or damages inter-ethnic unity; 5. Sabotages State religious policy or propagates heretical teachings or feudal superstitions; 6.Disseminates rumors, disturbs social order or disrupts social stability; 7. Propagates obscenity, pornography, gambling, violence, murder or fear or incites the commission of crimes; 8.Insults or slanders a third party or infringes upon the lawful rights and interests of a third party; 9.Includes other content prohibited by laws or administrative regulations. For further analysis of Chinese online content regulation see: Anne S.Y. Cheung. The Business of Governance: China's Legislation on Content Regulation in Cyberspace. New York University Journal of International Law and Politics, 2006, v. 38, p. 1-37 http://nyujilp.org/wp-content/uploads/2013/02/38.1_2-Cheung.pdf

as "blacklists" from authorities specifying what content needs to be either removed or blocked by the service itself.[543]

Baidu does not limit content restrictions to its home jurisdiction: the same search results that it restricts in China are also restricted for users anywhere in the world.[544]

Yandex: As discussed in Chapter 2, several Russian laws passed between 2012 and 2014 empower the government's executive branch to blacklist "extremist" content, content deemed harmful to minors, and copyright infringing content among other content without requiring a court order.[545] However in an interview for this report, Yandex executives insisted that the company does not filter or remove search results. Our researchers found no evidence to the contrary. In response to an e-mailed query, Yandex public relations manager Katerina Karnaukhova responded:

> "It is a fact and we are sad to confess that today in the Internet there are also materials that violate the law or ethical norms, but we still conduct our search all over the Internet and it is not our goal to edit or filter it. We do not block any information in our search results. If material is deleted from a website, it will also disappear from the search results."[546]

It is important to note that for content on other services beyond its search platform Yandex executives told our researchers in an interview that the company does receive and comply with content removal requests for other services such as video and photo hosting.

Google: The company's global reach has led it to adopt policies and practices that are both global but also sufficiently flexible so that the company can reach Internet users living in a vast array of different policy and legal contexts.

As a member of the Global Network Initiative, Google has made a commitment to interpret content removal demands from authorized authorities as narrowly as possible, and to challenge demands that appear incongruous with relevant law.[547] Google publishes information about its process for evaluating and responding to government and private

---

543 Interviewee wished to remain anonymous, date and location not disclosed for that purpose.

544 See Baidu is charged in U.S. for its online censorship. *The Wall Street Journal*. 19 May 2011. http://cn.wsj.com/gb/20110519/tec143847.asp (Accessed 16 June 2014) and Baidu and Chinese government are sued in New York for online censorship. 19 May 2011. http://www.bbc.co.uk/zhongwen/simp/chinese_news/2011/05/110519_baidu_lawsuit.shtml (Accessed 16 June 2014.)

545 Decree #1101 of the Government of the Russian Federation dated October 26, 2012. 'On the Uniform Automated Information System of the Russian Internet Blacklist.' English translation at: http://eais.rkn.gov.ru/docs.eng/1101.pdf; also see Courtney Weaver and Charles Clover, Russia's 'internet blacklist' sparks fears. FT.com. 11 July 2012. (Accessed 16 June, 2014) and Russian federal law 292521-6. Russian text at: http://www.copyright.ru/ru/library/zakonoproekti/pravovoe_regulirovanie_in/zakon_292521-6/; also see Monika Emert and Frederic Dubois. Russia: controversial anti-piracy law comes into force. Internet Policy Review. 1 August 2013. http://policyreview.info/articles/news/russia-controversial-anti-piracy-law-comes-force/185 (Accessed 16 June 2014.)

546 E-mail exchange with researcher Tatiana Indina, April 2014.

547 Global Network Initiative Implementation Guidelines. https://globalnetworkinitiative.org/implementationguidelines/index.php

demands to remove or filter content.[548] The company's "Transparency Report" (discussed in greater detail below and in the "Transparency" section 4.5 of this case study) indicates that it challenges or refuses to comply with a significant percentage of government requests around the world.[549] When it complies with a government request to restrict a piece of content in one jurisdiction, the content is restricted from view only in the jurisdiction where the request was made, unless the content also happens to violate the company's terms of service.[550] (In the case of European court decisions meant to apply to the entire European Union such as the 'right to be forgotten' case discussed later in this study, Google has interpreted this commitment to apply to its online properties across the EU but not beyond.) Child pornography, illegal in all jurisdictions, is one category of content that Google voluntarily and proactively removes from its search results without waiting for government requests.[551]

4.3.2 Self-regulation

Of the three search engines studied in this report, only Google uses its terms of service and internal policies to restrict a significant amount of content not prohibited by law. This is particularly true in the United States where the law restricts relatively little speech compared in comparison with the rest of the world. While some Google services such as YouTube and Google+ do not allow pornography, "graphic or gratuitous violence," and "hate speech," (though Blogger allows certain "adult content"),[552] Google considers its search engine to be its "least restrictive" of expression "because search results are a reflection of the content of the web."[553] Still, it does restrict and manipulate content globally in accordance with its terms of service and other internal policies. Examples include:

Sensitive personal information: Google excludes sensitive personal information such as 'sensitive government ID numbers, bank account and credit card numbers, and images

548 Controversial content and free expression on the web: a refresher. Official Google Blog. 19 April 2010. http://googleblog.blogspot.com/2010/04/controversial-content-and-free.html (Accessed 16 June 2014.)

549 Google Transparency Report. Requests to Remove Content. From Government. Summary of All Requests. https://www.google.com/transparencyreport/removals/government/

550 Google Transparency Report. Turkey. http://www.google.com/transparencyreport/removals/government/TR/ For example in the January-June 2013 reporting period: "We received 1,126 requests from government agencies to remove a total of 1,345 items from Blogger, Google+, and Web Search that the agencies claimed were in violation of law 5651. We removed 188 items that violated our product policies." Also see: Jeff Landale. Google transparency report sheds light on internet threats. 6 December 2012. https://www.accessnow.org/blog/2012/12/06/google-transparency-report-sheds-light-on-internet-threats (Accessed 15 April 2014.)

551 Ben Rooney. Microsoft, Google Join To Battle Child Porn. *Wall Street Journal*. 18 November 2013. http://online.wsj.com/news/articles/SB40001424052702304439804579205874211710440 (Accessed 15 April, 2014.)

552 "We do allow adult content on Blogger, including images or videos that contain nudity or sexual activity. But, please mark your blog as 'adult' in your Blogger settings. Otherwise, we may put it behind a 'mature content' interstitial." Google. Blogger Content Policy. https://www.blogger.com/content.g?hl=en (Accessed 4 May 2014.)

553 Rachel Whetstone. Controversial Content and Free Expression on the Web: A Refresher. Official Google blog. 19 April 2010. http://googleblog.blogspot.com/2010/04/controversial-content-and-free.html. (Accessed 4 May 2014.)

of signatures'[554] when users file removal requests.555 However, Google refuses such requests when it 'believe[s] someone is attempting to abuse these policies to remove other information from our results'.[556]

Penalties for prohibited search engine optimization techniques: Google penalizes websites that attempt to appear higher in search results by manipulating their website code or paying for links in a way that violates Google's search engine optimization policies. Several websites of reputable brands have been punished for this,[557] including WordPress,[558] the *Washington Post*,[559] the BBC[560] and Rap Genius.[561]

Spam and malware: Google search automatically, through algorithms and manual "demotion" of spam pages, penalizes pages that contain irrelevant content just to appear higher in ranking.[562] Google proactively shields users from spam and malware by displaying prominent warnings ('The Website Ahead Contains Malware!') when users click on bad links.[563] Yandex also protects its users by placing a warning message in search results next to websites that contain harmful code.[564]

Security of websites: As part of an effort to encourage website owners to strengthen their security practices, in August 2014 Google announced that its search algorithms would favor websites that use HTTPS encryption by default, thus shielding the user's

554 Google. Inside Search – Policies. https://www.google.com/insidesearch/howsearchworks/policies.html

555 Google. Search Help – Removal Policies. https://support.google.com/websearch/answer/2744324?hl=en (Accessed 1 July 2014); and Sheily Chhabria. 'Protecting Consumers From Identity Theft and Scams'. Google Public Policy Blog. 5 March 2014. http://googlepublicpolicy.blogspot.com/2014/03/protecting-consumers-from-identity.html (Accessed 1 July 2014.)

556 Google. Search Help – Removal Policies. https://support.google.com/websearch/answer/2744324?hl=en

557 Danny Sullivan. 10 Big Brands That Were Penalized By Google, From Rap Genius To The BBC. *Marketing Land*. 12 February 2014. http://marketingland.com/10-big-brands-that-were-penalized-by-google-69646 (Accessed 2 May 2014.)

558 Andy Baio. Wordpress Website's Search Engine Spam. Waxy blog. 30 March 2005. http://waxy.org/2005/03/wordpress_websi (Accessed 1 July 2014.); and Matt Mullenweg. A Response. 1 April 2005. http://ma.tt/2005/04/a-response (Accessed 1 July 2014.)

559 Shawn Smith. Google takes Washington Post, news sites and popular blogs down a notch. New Media Bytes. 24 October 2007. www.newmediabytes.com/2007/10/24/google-takes-washington-post-news-sites-and-popular-blogs-down-a-notch (Accessed 1 July 2014.)

560 Barry Schwartz. Google Penalized One Article On BBC's Web Site. *Search Engine Land*. 18 March 2013. http://searchengineland.com/google-penalized-one-article-on-bbcs-web-site-151954 (Accessed 29 April 2014.)

561 Lydia Laurenson. Google, Censorship, and Salesmanship: The Epic Smackdown of RapGenius. *Medium: Futures Exchange*. 22 January 2014. https://medium.com/futures-exchange/b0c49f6853ca (Accessed 3 May 2014.); Leslie Kaufman. Google Penalizes Rap Genius for Gaming Search Rank. *New York Times*. 26 December 2013. www.nytimes.com/2013/12/26/business/media/google-penalizes-rap-genius-for-gaming-search-rank.html (Accessed 3 May 2014.)

562 Google. Inside Search – Fighting Spam. https://www.google.com/insidesearch/howsearchworks/fighting-spam.html (Accessed 3 May 2014.)

563 Sheily Chhabria. Protecting Consumers From Identity Theft and Scams. Google Public Policy Blog. 5 March 2014. http://googlepublicpolicy.blogspot.com/2014/03/protecting-consumers-from-identity.html (Accessed 1 July 2014.)

564 Yandex. Identifying potentially harmful sites. http://help.yandex.com/search/beware/harmful-sites.xml

activity on the website from interception (although a web browser as well as tracking cookies may still record and transmit information about websites visited).[565]

4.3.3 Features particular to search engines

In addition to the main search results, all three search engines studied include other features unique to search engines that can be subject to manipulation or restriction in distinct ways:

Search query prediction: Google, Baidu, and Yandex all offer a feature known as "autocomplete" or "word completion" which automatically generates suggested word combinations after the user types in the first letters or words of a search. All three services exclude certain words and phrases from this function. Baidu and Yandex exclude predictions that would lead the users to content that is illegal under Chinese or Russian law, respectively.[566] Google excludes the same categories of content that it restricts on its social media platforms as well as "predictions about activities that could result in real-world physical harm", such as human trafficking; sale of drugs, weapons or other illegal goods and services; and "illegal and dangerous activities, like assault and suicide."[567]

Search-word related advertising: All three search engines studied display advertising alongside relevant search terms. Baidu and Yandex apply domestic legal standards.[568] Google restricts a broader range of content than U.S. law requires for its AdWords service that displays advertisements alongside search results linked to particular words. For example, speech that constitutes "attempts to revise history against the interests of a protected group" is constitutionally protected in the United States but is prohibited in Google Adwords because it is illegal elsewhere. Google cites legal regulations alongside its goal "to ensure a positive user experience, and to protect Google's brand" as reasons for its global restrictions on hate speech in AdWords.[569]

Parental controls: Google's SafeSearch feature allows users to voluntarily choose settings that filter adult content (regardless whether it is legal or illegal in their home jurisdiction) from search results. Google maintains a manually curated "whitelist" for misidentified websites (such as essex.edu, for example) to prevent them from being classified as

565 Google to prioritise secure sites. 7 August 2014. http://www.bbc.com/news/technology-28687513; and HTTPS as a ranking signal. Google Webmaster Central Blog. 6 August 2014. http://googlewebmastercentral.blogspot.com/2014/08/https-as-ranking-signal.html (14 August 2014.)

566 The application of autocomplete in a Baidu search box. Baidu Alliance User Experience Center. http://ueo.baidu.com/?p=2325 (Accessed 16 June 2014.) This guidance specifies that 'Baidu Suggest will filter politics and pornography'. Also see Yandex corporate principles. http://company.yandex.ru/rules

567 Yandex corporate principles, op. cit.. And Yandex code of corporate ethics. http://company.yandex.ru/rules/code/

568 For example, search 'free vpn' on Baidu, there will be little advertising along the right side of search results. Above the results, there is a warning: 'According to relevant laws and policies, part of the search results is not shown.' Experiment conducted by the report's China researcher. 30 June 2014. Also see Yandex corporate principles and Yandex code of corporate ethics, op. cit.

569 Google Advertising Policies support. Offensive or inappropriate content. https://support.google.com/adwordspolicy/answer/175902?hl=en&ref_topic=1626336

pornography.[570] In some jurisdictions Google turns on SafeSearch by default.[571] Yandex offers a similar optional service called 'family search'. By default Yandex filters adult content that is not specifically sought (no adult content will appear when simply entering general terms like 'videos'), though this 'moderate' filter setting can also be disabled.[572]

4.3.4 Implementation in national context

China

Baidu displays a mix of compromise and pragmatism in the face of strict liability combined with broad laws and regulations. Baidu's algorithm is programmed to block results containing words and phrases that appear on the government blacklists, along with entire websites that the company is instructed to remove from its search database. The volume and nature of government requests is not officially disclosed. However, some overseas-based websites[573] and news media[574] have obtained and published lists of sensitive words and topics that companies have received. In 2009 the U.S.-based website *China Digital Times* published a set of documents leaked by a Baidu employee.[575] Based on an analysis of these leaked materials combined with stakeholder interviews, the restricted words, phrases, and Web addresses can be divided into the following categories:

- Names of the Chinese high leadership
- Protests and dissident movements
- Events, places and people deemed politically sensitive
- Foreign websites and organizations blocked at the network level
- Other (pornography, etc.)

Researchers have found that most of the instructions to remove or block specific content from search results are communicated on a "just in time" basis: as warranted by breaking

---

570 Google. Inside Search – Policies. op. cit.

571 Testing conducted by the report's China researcher confirmed that SafeSearch feature could not be deactivated on Google.com.hk. 30 June 2014.

572 Yandex. Filtering adult content. http://help.yandex.com/search/beware/adult-filter.xml More elaborate Russian explanation at http://company.yandex.ru/rules/filtration.

573 Censorship of keywords in China. Greatfire.org. https://en.greatfire.org/search/keywords. Berkeley-based *China Digital Times* operates an Open-Sourced Research on Blacklisted Search Keywords on Sina Weibo, http://chinadigitaltimes.net/chinese/category/%E7%BD%91%E6%83%85%E9%80%8F%E8%A7%86/%E6%95%8F%E6%84%9F%E8%AF%8D%E5%BA%93/.

574 Keywords Used to Filter Web Content. *Washington Post*, 18 February 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/02/18/AR2006021800554html/ (Accessed 25 June 2014.)

575 Baidu's Internal Monitoring and Censorship Document Leaked (1) (Updated). China Digital Times. 30 April 2009. http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked/; Baidu's Internal Monitoring and Censorship Document Leaked (2). China Digital Times. 29 April 2009. https://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked-2/ ; Baidu's Internal Monitoring and Censorship Document Leaked (3). China Digital Times. 28 April 2009. http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked-3/ (Accessed 25 June 2014.)

news and other "sudden incidents"- accidents, natural disasters, corruption scandals, etc. - that may trigger strong responses from Chinese "netizens." Such restrictions are often limited to a specific period of time rather than permanent.[576] One lawyer interviewed for this report who has been involved with cases involving online content observed that authorities increasingly communicate instructions by phone instead of in writing.[577]

According to one industry executive, Baidu would seem sometimes to ignore requests from local government authorities whose concerns and priorities are not shared by central authorities. While it reportedly pro-actively restricts content known to be a concern to central authorities, Baidu seems likely to wait for a government demand rather than pro-actively remove "relatively obscure" politically sensitive information, particularly around emerging incidents in remote locations far from Beijing.

Despite the frequent and often extensive demands placed on companies to restrict content, even a domestic critic of the government's approach to regulating the Internet described search engines like Baidu as a "positive force" for freedom of expression. "There is some space for information to be spread before the supervising departments catch up and tag it as sensitive," one entrepreneur and industry veteran said in an interview. "After all, the Internet companies are private businesses. So in order to attract clicks, they do their best to provide fast and objective information." [578]

Since 2010, **Google** no longer operates a search service within Chinese jurisdiction and no longer complies with Chinese government requests to restrict search results.[579] As of early August 2014 the front page of Google search, including google.com and its Hong Kong-based search engine google.com.hk, was filtered in China.[580]

576 Internet censorship listed: how does each country compare? *The Guardian.* 16 April 2014. http://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list (Accessed 26 June 2014.)
577 Interviewee wished to remain anonymous, date and location not disclosed for that purpose.
578 Interviewee wished to remain anonymous, date and location not disclosed for that purpose.
579 After short revival, Google service disruptions in China return. Reuters. 11 July 2012. http://in.reuters.com/article/2014/07/11/google-china-idINKBN0FF1DO20140711 (Accessed 10 July.)
580 Abby Liu. Just Google It? Not In China, Where Google Remains Blocked. 18 June 2014. http://globalvoicesonline.org/2014/06/18/china-google-censorship-tiannamen-block/ (Accessed 10 July.)

BOX: Google Search in China, 2006-2010

In January 2006 Google launched a search engine operated from within China, Google.cn. Between 2006 and 2010 Google.cn was not subject to network-level filtering because it complied with government requirements to restrict its search results. This enabled Google to compete more effectively for Chinese users with Baidu, whose search results are rarely subject to ISP-level filtering because the company restricts its search results in accordance with government instructions. Then in early 2010, in the wake of a large-scale cyber-attack, Google's U.S.-based management decided to re-locate Google.cn to Hong Kong, whose legal system is separate from the rest of China. After the relocation, China-based users of Google.cn experienced frequent outages triggered by the network-level filtering of search results containing sensitive words. This resulted in a sharp drop in Google's market share, and corresponding boost to Baidu's market share. Then in June 2014, Google search became almost completely inaccessible to Chinese users with the exception of Hong Kong and remained so at the time of this report's writing.

India

Google receives and responds to numerous requests for the removal of search results in response to governmental and law enforcement requests as well as court orders. At times, Google restricts access to content based on these requests. For example, in 2012 Google restricted access to the film "Innocence of Muslims" in India as well as a number of other countries.[584] Also in 2012, Google received a court order for the removal of 247 search results linking to websites that allegedly violated individuals' privacy. Google did not remove the search results as the relationship between the results and the court order were unclear.[585] Between January and June 2012, based on court orders Google removed 360 search results linking to webpages containing adult content that allegedly violated individuals' privacy.[586] According to Google's Transparency Report, the types of content that have been requested for removal since July 2010 in India include: defamation, religious offense, privacy and security, impersonation, adult content, hate speech, bullying/harassment, copyright, government criticism, national security, geographical dispute, and information that falls in the category of 'other'.

In the January to June 2013 transparency reporting period, requests for removal of defamatory content from the Google search platform were at their highest, with requests for removal of content that constituted impersonation, adult content, and religious offense following. For the same reporting period, requests for removal of content on Google's

581 Google to censor China Web searches. 24 January 2006. CNet.com. http://news.cnet.com/Google-to-censor-China-Web-searches/2100-1028_3-6030784.html (Accessed 16 June 2014.)
582 Google angers China by shifting service to Hong Kong. 23 March 2010. *The Guardian.* http://www.theguardian.com/technology/2010/mar/23/google-china-censorship-hong-kong (Accessed 16 July 2014.)
583 Google Losing Ground in China. 31 March 2011. *The Wall Street Journal.* http://online.wsj.com/news/articles/SB10001424052748704530204576234693138486996 (Accessed 16 July 2014.)
584 Google Transparency Report. India- Requests to remove content. Government Requests. July – December 2012. http://www.google.com/transparencyreport/removals/government/IN/?p=2012-12
585 Google Transparency Report. India- Requests to remove content. Government Requests. July – December 2012. http://www.google.com/transparencyreport/removals/government/IN/?p=2012-12
586 Google Transparency Report. India- Requests to remove content. Government Requests. January – June 2012. http://www.google.com/transparencyreport/removals/government/IN/?p=2012-06

image search included adult content, defamatory content, and content impacting individual privacy and security. On the Google web search autocomplete, defamatory content was affected the most.[587] This is in contrast to the July - December 2012 reporting period, where Google web search received the highest number of removal requests for content infringing on privacy and security.[588]

Russia

As noted in the previous section, **Yandex** executives claim that the search engine does not restrict search results because illegal websites are already filtered by the ISPs. In April 2014, the Duma passed the so-called "blogger law," requiring bloggers with more than 3,000 visitors per day to register with the government as media. Such "popular bloggers" would also be required to use their real names and adhere to mass media regulations. In response, Yandex shut down a feature of its blog search that displayed ratings and readership figures, claiming that the numbers were not entirely accurate.[589] This step served to shield popular bloggers who did not register.

Google reports that it removes some search results at the request of the Russian government, documenting what requests it has received and complied with through its Transparency Report. (which will be discussed in greater detail in the "Transparency" section of this case study). For the January to June 2013 reporting period, Google received one court order and three other orders categorized as "executive, police etc" to remove four results. The company complied with all four orders, three of which were related to "suicide promotion," a content category prohibited under Russian law, while the fourth request was unspecified. In 2012 Google received and complied with one request described as being related to "national security" and two requests described also as "suicide promotion." [590]

In Russia, both Yandex and Google lobbied against the Antipiracy law (Bill N° 292521), passed in 2013, that makes it illegal to spread content in a way that violates copyright.[591] Both companies oppose the law in its current form because it maximizes opportunities for accidental over-blocking which affects websites that are not infringing copyright or otherwise illegal. Google advocates that Russia should adopt a DMCA-style "notice and takedown" approach (despite its noted flaws in the United States, as discussed below), whereby the party whose copyright is infringed directly notifies the company hosting the content of the infringement. Industry interviewees told our researchers that Google is

587 Google Transparency Report. India - Requests to Remove Content. Summary of All Requests. Government Requests. January – June 2013. http://www.google.com/transparencyreport/removals/government/IN/

588 Google Transparency Report. India - Requests to Remove Content. Government Requests. Product Breakdown. January – June 2012. https://www.google.com/transparencyreport/removals/government/IN/?metric=compliance&by=product&p=2012-12

589 «Яндекс» закрыл рейтинг популярности блогеров [Yandex has closed popularity blogger ratings] Lenta.ru, April 18, 2014, http://rt.com/politics/155580-russia-internet-blogger-bill/http://lenta.ru/news/2014/04/18/blogi1/

590 Google Transparency Report. Russia. Requests to Remove Content. Government Requests. By Product. January-June 2013. https://www.google.com/transparencyreport/removals/government/RU/?by=product (Accesssed 28 June 2014.)

591 Russian federal law 292521-6. op. cit.

appealing to copyright owners in Russia to take their complaints directly to the company hosting the content in order to avoid government involvement that could lead to broader filtering. Yandex representatives, on the other hand, stated in interviews that the company chooses not to act as a mediator for online content issues, including copyright issues.

In July 2014 the Russian parliament enacted a new law requiring foreign internet companies to store personal data of Russian users within the country. The law originally set an implementation deadline of January 1, 2016 but in September the parliament moved the deadline to January 1, 2015.[592] The law has been interpreted in the international media to mean that foreign intermediaries might be filtered by Russian ISPs if they fail to comply. Since it is possible to provide search service without collecting any user data, it remains unclear how Google search will be affected by this law. (Other Google services such as GMail and YouTube which do store large quantities of user data and content as part of their core services, seemed more likely as of this writing to be affected, although those services are not within the scope of this study.)[593]

The United States

Most of the instances in which Google restricts search results globally are to comply with copyright law. In fact, copyright takedown notices are responsible for 95 per cent of the takedown requests Google receives for search results, and it complies with 97 per cent of them.[594] However, critics point out that the DMCA copyright takedown system in the U.S. (discussed in the "Intermediary liability" section of Chapter 2) incentivizes search engines to promptly remove content rather than question requests, because the penalties for the search engine can be astronomical: up to $150,000 per infringement.[595] This can have a negative impact on freedom of expression because the DMCA system makes it easy for those who want content to be removed from the Internet to abuse the system by claiming copyright infringement.[596]

---

592 Sergei Blagov. Russia Seeks New 'Impossible' Deadline For Server Localization of Jan. 1, 2015. Bloomberg. 8 September 2014. http://www.bna.com/russia-seeks-new-n17179894570/ (Accessed 2 October 2014.)

593 Paul Sonne and Olga Razumovskaya. Russia Steps Up New Law to Control Foreign Internet Companies. The Wall Street Journal. 24 September 2014. http://online.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920?cb=logged0.07114209281280637 (Accessed 2 October 2014.)

594 How Google Fights Piracy. September 2013. p. 16. https://docs.google.com/a/google.com/file/d/0BwxyRPFduTN2dVFqYml5UENUeUE/edit

595 Mitch Stoltz. To Safeguard the Public Domain (and the Public Interest), Fix Copyright's Crazy Penalties. EFF Deeplinks blog. 18 January 2014. https://www.eff.org/deeplinks/2014/01/safeguard-public-domain-and-public-interest-fix-copyrights-crazy-penalties (Accessed 15 April 2014.)

596 Daniel Seng. The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices. 20 March 2014. Virginia Journal of Law and Technology, Forthcoming. Available at SSRN: http://ssrn.com/abstract=2411915 or http://dx.doi.org/10.2139/ssrn.2411915; Also see Takedown Hall of Shame. Electronic Frontier Foundation. https://www.eff.org/takedowns (Accessed 9 August 2014.)

sGoogle says that it receives "inaccurate or unjustified copyright removal requests for search results that clearly do not link to infringing content," noting that it does not comply with such requests. In 2012 Google's Fred von Lohmann wrote: "We've also seen baseless copyright removal requests being used for anticompetitive purposes, or to remove content unfavorable to a particular person or company from our search results."[597] Google sometimes takes a stand against the requests. For example in 2013, Google refused to remove from its search results "The Pirate Bay" home page - the Pirate Bay website's individual pages may infringe copyright, but the home page itself does not host any copyright-infringing content.[598]

In 2012, Google's algorithms were reprogrammed to support the DMCA system: The company announced websites that receive high numbers of "valid copyright removal notices…may appear lower in our results." The purpose, according to an official Google blog post, is to "help users find legitimate, quality sources of content more easily."[599]

BOX: Impact of domestic website restrictions on global search

In 2012, the software engineer and writer David Auerbach wrote of problems caused by algorithms that "do not arise from malicious intent, but from expediency and happenstance."[600] Companies that operate search engines are learning that applying an inherently apolitical mathematical algorithm to a heavily manipulated and filtered corpus of websites can be harmful to freedom of expression.

In early 2014 the activist group GreatFire accused Microsoft Bing of extending its Chinese-language content restriction practices required for its operation inside China to users located in other jurisdictions where the same laws and requirements do not apply. The activists pointed to a comparison of Google's Chinese language search results for terms considered politically sensitive in China, versus Bing's Chinese-language search results – in both instances when the search is conducted from jurisdictions such as the United States and the UK. While Google's results contained content from many web pages that are filtered or otherwise inaccessible in China, Bing's results contained mainly content from websites created and operated from within China – and which are therefore subject to Chinese laws and regulations. Microsoft responded that it "does not apply China's legal requirements to searches conducted outside of China."[601]

---

597 Fred von Lohmann. Transparency for Copyright Removals in Search. Official Google Blog. 24 May 2012. http://googleblog.blogspot.com/2012/05/transparency-for-copyright-removals-in.html (Accessed 9 August 2014.)

598 Ernesto Van Der Sar. Google Refuses to Move the Pirate Bay Homepage. TorrentFreak blog. 9 September 2013. http://torrentfreak.com/google-refuses-to-remove-the-pirate-bay-homepage-130909 (Accessed 2 April 2014.)

599 An update to our search algorithms. Google Inside Search blog. 8 October 2012. http://insidesearch.blogspot.com/2012/08/an-update-to-our-search-algorithms.html (Accessed 2 April 2014.)

600 David Auerbach. The Stupidity of Computers. Issue 13: Machine Politics. Winter 2012. http://nplusonemag.com/issue-13/essays/stupidity-of-computers/ (Accessed 2 April 2014.)

601 Microsoft, Bing Censor Chinese Search Results System Error. *The Guardian*. 12 February 2014. www.theguardian.com/technology/2014/feb/12/microsoft-bing-censor-chinese-search-results-system-error (Accessed 9 April 2014.)

In the opinion of one member of this report's research team who has studied the issue of search engines and freedom of expression over the past decade, the problem is more likely due to the fact that search ranking relies on calculating inbound links as well as user "click through" rates to a website. Due to the massive size of the Chinese internet (618 million users as of December 2013),[602] incoming links and click-throughs for the websites that rank highly on Chinese search engines are orders of magnitude greater than click-throughs for websites popular with the West. The number of people clicking through to simplified Chinese language websites based outside of China - particularly if they are filtered within the country - is inevitably, and substantially, lower.

It appears that Google's search algorithm was adjusted to compensate for this imbalance created by jurisdiction-specific filtering, but as of early 2014, Bing's had not.[603] This incident speaks to an emerging challenge to freedom of expression and access to information on search engines—content restriction within a large country has the potential to affect speakers of that country's primary language regardless of where they live. This can apparently be prevented only if the search engine operator identifies and compensates for lower click-through rates and inbound links that are intrinsically a feature of websites that are filtered.

4.3.5 Europe and the "Right to Be Forgotten"

As many of the examples in this case study have illustrated, search engines—even when operating in legal environments where freedom of expression receives strong protection — are not entirely neutral arbiters of information. Adjustments are made globally to the search algorithm in order to protect users from spam and malware or identity theft, to protect children from sexual exploitation, and to comply with intellectual property law. Many more adjustments are made in response to private and government requests in specific jurisdictions around the world. The role of search engines now faces a further set of challenges in Europe – and potentially around the world – with the European Court of Justice's May 13, 2014 ruling, establishing the "right to be forgotten" throughout the European Union.

A previous UNESCO report, published in 2012, highlighted the inherent tensions between privacy and freedom of expression.[604] One of many potential tensions is between the individual's desire to eliminate negative information about him or herself from the Internet and the right of others to receive and impart information.[605] On 13 May 2014, the Court of Justice of the European Union (CJEU) ruled in the case *Google Spain v AEPD,* brought against Google by a Spanish man who argued that an auction notice of his repossessed

602 According to a January 2014 report by the China Internet Network Information Center (CNNIC). www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201401/P020140116395418429515.pdf; Steven Millward. 16 January 2001. China Now Has Half a Billion Mobile Web Users, 618 Million Total Internet Users. *Tech in Asia*. www.techinasia.com/cnnic-china-500-million-mobile-web-users-and-618-internet-users-2013 (Accessed 9 April 2014.)

603 Rebecca MacKinnon. 14 February 2014. Where is Microsoft Bing's Transparency Report? *The Guardian.* http://www.theguardian.com/commentisfree/2014/feb/14/micorsoft-bing-china-censorship-transparency (Accessed 9 April 2014.)

604 Mendel et. al., op. cit. p. 97-104.

605 Global Network Initiative. 15 May 2014. EU Court 'Right to Be Forgotten' Ruling Threatens Freedom of Expression. http://www.globalnetworkinitiative.org/news/eu-court-%E2%80%98right-be-forgotten%E2%80%99-ruling-threatens-freedom-expression

home appearing in Google's search results constituted a violation of his right to privacy. 606 According to the court's ruling, Internet users in Europe now have the right to demand that search engines remove links to web pages about them that are 'inadequate, irrelevant or excessive in relation to the purposes of the processing'.[607] Furthermore, the individual's right to privacy overrides 'as a general rule' the public's interest in finding information. At the same time, the public interest may be preponderant, for example in the cases of public figures.[608]

The ruling came under heavy criticism from free expression groups such as Article 19, the Committee to Protect Journalists and Index on Censorship, who warned that excessive enforcement of privacy rights can impinge on press freedom.[609] This position aligns with one that recognises that press freedom represents the right to use free expression to communicate with the wider public, and that while removing links to content does not per se violate the original expression, it eliminates much of the significance of publishing in the digital age.

Other digital rights advocates argued that media coverage and the free expression community overreacted. For example, Joe McNamee, director of the European Digital Rights Initiative, pointed out that contrary to some press reports Google had 'not been asked to delete data', merely block the link from appearing in search results for searches on the name of the person in question.'[610] Some also pointed out that the search engine operator is given a great deal of discretion in responding to individual requests, and is not compelled to remove any results prior to a court ruling. Jef Ausloos of the University of Leuven said that upon closer inspection 'much of the wording seems to be very nuanced and limited in scope'.[611]

---

606 Europe's top court: people have right to be forgotten on Internet. Reuters. 13 May 2014. http://www.reuters.com/article/2014/05/13/eu-google-dataprotection-idUSL6N0NZ23Q20140513 (Accessed 14 July 2014.)

607 Read original CJEU ruling at Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [2014] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131; For additional commentary see David Streitfeld. 'European Court Lets Users Erase Records on Web'. *New York Times*. 14 May 2014. www.nytimes.com/2014/05/14/technology/google-should-erase-web-links-to-some-personal-data-europes-highest-court-says.html (Accessed 24 June 2014.)

608 CJEU ruling, op. cit.

609 Geoffrey King. EU 'right to be forgotten' ruling will corrupt history. Committee to Protect Journalists. 4 June 2014. http://cpj.org/blog/2014/06/eu-right-to-be-forgotten-ruling-will-corrupt-histo.php; Index urges court to rethink ruling on "right to be forgotten". Index on Censorship. 30 May 2014. http://www.indexoncensorship.org/2014/05/index-urges-court-rethink-ruling-right-forgotten/; Gabrielle Guillemin A right to be forgotten? EU Court sets worrying precedent for free speech. 14 May 2014. http://www.article19.org/join-the-debate.php/146/view/ (Accessed 24 June 2014.)

610 Joe McNamee. Google's right to be forgotten – industrial scale misinformation? European Digital Rights Initiative. 9 June 2014. http://edri.org/forgotten (Accessed 24 June 2014.) McNamee links to the following two articles; Victoria Espinel. 'Coming Together to Combat Online Piracy and Counterfeiting'. White House Office of Management and Budget's 'OMBlog'. 15 July 2013. www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting (Accessed 24 June 2014.); and Bad Google DMCA Takedown Is Hurting Us, Hosting Site Says. TorrentFreak. 30 March 2014. https://torrentfreak.com/bad-google-dmca-takedown-is-hurting-us-hosting-site-says-140330 (Accessed 24 June 2014.)

611 Jef Ausloos. 13 May 2014. European Court Rules against Google, in Favour of Right to be Forgotten. London School of Economics and Political Science. Media Policy Blog. http://blogs.lse.ac.uk/mediapolicyproject/2014/05/13/european-court-rules-against-google-in-favour-of-right-to-be-forgotten (Accessed 24 June 2014.)

By the end of May 2014, Google came up with a 'rudimentary framework' for compliance with the ruling and to cover itself from subsequent cases based on the ruling. It created a public web page[612] through which users based in Europe could request that their names be decoupled from certain search results.[613] The removals would only take place on Google search websites specific to the European Union (google.co.uk or google.co.de, for example) and would remain visible on the global search engine, Google.com. A notification that such removals had taken place would appear on the search results page.[614]

As a member of the Global Network Initiative, Google faced the need to reconcile compliance with the ruling with its GNI commitments to be transparent about how content is restricted, as well as to interpret official requests around content restriction as narrowly as possible.[615] On 11 July 2014 Google reported that it had received 70,000 restriction requests covering 250,000 websites since mid-May. The requests were being reviewed manually, and the company had also instituted a policy of notifying websites when one of their pages was removed.[616] *The Guardian* newspaper was one of the first news organizations to receive notifications that links to some of its stories had been removed from its search results in the EU.[617] Wikipedia's founder Jimmy Wales condemned the process as "censorship" after his organization received notice that several links to Wikipedia content had been removed in compliance with requests from people who were the subject of that content.[618]

Google also set up an advisory council to investigate how it should balance privacy and freedom of expression. Senior Vice President and Chief Legal Officer David Drummond wrote that while some requests were clearly illegitimate, like politicians seeking to cover up prior misdeeds, one could sympathize with many others:

> …from the man who asked that we not show a news article saying he had been questioned in connection with a crime (he's able to demonstrate that he was never charged) to the mother who requested that we remove news articles for

612 Google. Search removal request under European Data Protection law. https://support.google.com/legal/contact/lr_eudpa?product=websearch (Accessed 24 June 2014.)

613 Mark Scott. 18 June 2014. Google Ready to Comply With "Right to Be Forgotten" Rules in Europe. *New York Times*. http://bits.blogs.nytimes.com/2014/06/18/google-ready-to-comply-with-right-to-be-forgotten-rules-in-europe (Accessed 24 June 2014.)

614 Danny Sullivan. 30 May 2014. How Google's New "Right To Be Forgotten" Form Works: An Explainer. Search Engine Land. http://searchengineland.com/google-right-to-be-forgotten-form-192837 (Accessed 24 June 2014.)

615 Global Network Initiative Implementation Guidelines. Freedom of Expression. http://globalnetworkinitiative.org/implementationguidelines/index.php#29 and Global Network Initiative Principles. Freedom of Expression. http://globalnetworkinitiative.org/principles/index.php#18

616 Searching for the right balance. Google Official Blog. 11 July 2014. http://googleblog.blogspot.com/2014/07/searching-for-right-balance.html

617 James Ball. 10 July 2014. Google admits to errors over Guardian 'right to be forgotten' link deletions. *The Guardian.* http://www.theguardian.com/technology/2014/jul/10/google-admits-errors-guardian-right-to-be-forgotten-deletions (Accessed 14 August 2014.)

618 Alex Hern. 6 August 2014. Wikipedia swears to fight 'censorship' of 'right to be forgotten' ruling. *The Guardian.* http://www.theguardian.com/technology/2014/aug/06/wikipedia-censorship-right-to-be-forgotten-ruling (Accessed 14 August 2014.)

her daughter's name as she had been the victim of abuse. It's a complex issue, with no easy answers.[619]

In the third quarter of 2014, the company was scheduled to hold public consultation sessions across Europe, and had also published an online questionnaire seeking public comment.[620] Questions included: "What is the nature and delineation of a public figure's right to privacy?" and "How should we differentiate content in the public interest from content that is not?" and "Does the public have a right to information about the nature, volume, and outcome of removal requests made to search engines?"[621]

Meanwhile, as of June 2014, it appeared that the CJEU ruling might effect similar changes around the world. For example, privacy regulators attending the Asia Pacific Privacy Authorities (APPA) forum on 17–18 June 2014 in Seoul, Korea, discussed the possibility of 'engaging with Google and other search engines' and said that they would be publishing a report with recommendations on this topic by the next APPA meeting in December.[622] The implications of implementing similar rules in other jurisdictions began to come under debate. For example, in an editorial in a local newspaper, Prof. Park Kyung-Sin of Korea University Law School expressed concern that legislation of the right to be forgotten this could grant broad license to national authorities to censor online content.[623]

4.4 Data retention, collection, and surveillance

The retention of user data by search engines combined with heightened knowledge about government surveillance practices appears to have affected the public's trust in search engines. An analysis of publicly available Google (Search) Trends data before and after June 2013 (when former NSA contractor Edward Snowden began to release his revelations about U.S. government surveillance via Internet intermediaries) sought to find "empirical evidence of a chilling effect on users' willingness to enter [sensitive] search terms."[624] They examined search traffic data for 282 terms in 11 countries that included China and Russia (but not India).[625] Nine out of eleven countries exhibited a decrease in search traffic for terms that were rated as "likely to get you in trouble with the U.S.

619 Searching for the right balance. op cit.

620 Lance Whitney. 30 July 2014. Google seeks public opinion on 'right to be forgotten'. CNet. http://www.cnet.com/news/google-seeks-public-opinion-on-right-to-be-forgotten/ (Accessed 14 August 2014.)

621 Google. Formal request for public comment and evidence. https://services.google.com/fb/forms/advisorycouncilcomments/

622 Asia Pacific Privacy Authorities. 41st APPA Forum – Communiqué. www.appaforum.org/resources/communiques/41stforum.html (Accessed 24 June 2014.)

623 Park Kyung-Sin. 8 August 2014. A 'surveillance' right to be forgotten. *Hangyerye* http://www.hani.co.kr/arti/opinion/column/650266.html (Accessed 10 August 2014.) With thanks to Jae Yeon Kim for bringing this article's to the authors' attention.

624 Alex Marthews and Catherine Tucker. 24 March 2014. Government Surveillance and Search Behavior. SSRN. http://ssrn.com/abstract=2412564.

625 According to the United States and its top ten international trading partners according to the U.S. Census for the 2012–13 trading year. These were, in order, Canada, China, Mexico, Japan, Germany, South Korea, the UK, France, Brazil, and Saudi Arabia. Tucker and Marthews op. cit. p.3.

government," but an increase for terms "not likely to get you in trouble." In the United States, the magnitude of this drop was 2.2 per cent.[626]

As noted earlier, in the United States, the PEN American Center survey of 520 American writers found a chilling effect.[627] Even before the surveillance revelations, a February 2012 Pew Internet & American Life survey found that Americans were not only "anxious about the collection of personal information by search engines," but 62 per cent of them also did "not know how to limit the information that is collected about them."[628]

Similar surveys have not been conducted in Russia and China that would provide parallel data about levels of public understanding of data retention and collection by search engines, or levels of public awareness about the nature and extent of government surveillance. Nonetheless the studies cited above do indicate that at least in some societies, awareness of the lack of privacy and existence of some level of pervasive surveillance can have a chilling impact on search engine users' freedom of expression.

Concerns about data collection by search engines (and other online services) have prompted the rise of alternatives that claim not to track or store users' digital data.

4.4.1 Company policies and practices

General Privacy Policies

All three companies have privacy policies with varying degrees of specificity. Of the three, only Google is subject to regular third-party privacy audits, in accordance with a 2011 ruling by the U.S. Federal Trade Commission.[629]

Google's Privacy Policy (unified for all of the company's services) states that it collects "log information," including "details of how you used our service, such as your search queries."[630] This information also includes user IP addresses, hardware information of the mobile device they may be searching from (if applicable) and "cookies that may uniquely identify your browser or your Google Account." This is done, the company says, to provide, maintain, protect and improve its services, to develop new services, "to protect Google and our users," and "to offer you tailored content - like giving you more relevant search results and ads."[631] The **Yandex** privacy policy is called a 'Confidentiality Policy,' and describes what kinds of data the company collects and for what purpose.

---

626 Excepting Saudi Arabia and South Korea. See Tucker and Marthews, op. cit. p.14.

627 PEN American Center. Chilling Effects: NSA Surveillance Drives Writers to Self-Censor. November 2013. www.pen-international.org/read-pen-american-centres-report-chilling-effects-nsa-surveillance-drives-writers-to-self-censor (Accessed 2 May 2014.)

628 Kristen Purcell, Joanna Brenner, and Lee Rainie. 9 March 2012. Search Engine Use 2012. Pew Internet & American Life Project. www.pewinternet.org/2012/03/09/search-engine-use-2012.

629 Federal Trade Commission. 30 March 2011. FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network. http://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz

630 Google. Privacy Policy. Privacy & Terms. https://www.google.com/policies/privacy/

631 Google. Key Terms. Privacy & Terms. https://www.google.com/intl/en/policies/privacy/key-terms/

Yandex says it gathers such information necessary for reasons including development of new services, to improve quality of service and for targeted advertisements.[632] In its Privacy Policy **Baidu** states that it collects users' personal information, log information, equipment information, cookies and anonymous identifiers. It explains the purpose of gathering information and promises to store and process the information anonymously.[633]

Data Retention

Google does not disclose how long it retains user data or what data is "anonymized" (de-linked from data that would enable re-identification of the user).[634] While Google logs search history by default, users can delete their history manually by accessing Google Dashboard. Users can also disable logging of their Web browsing history when logged in.[635] Like Google, **Yandex** also provides users with the option to delete their Web history or opt out of the storage of their Web history.636 Company executives at Yandex have stated publicly that user data will be stored for at least three months, although that information was not found on the company's own website.[637] **Baidu** does not offer a similar feature to delete search history, and makes no commitment about a time limit for storing such information.[638]

Security and encryption

In March 2014 Google announced that it was implementing encryption by default for all web searches worldwide.[639] Such encryption limits the ability for third parties to inconspicuously intercept search terms entered by the user. However, Google notes that "when you visit another website from the Google search results page, that website may be able to identify what site you came from or the search terms that you used."[640] Yandex offers encrypted search on Yandex.com but not Yandex.ru. Baidu does not offer encrypted search.

Disclosure of User Data to Government Authorities

Yandex company representatives have stated that the company does not share user information with third parties with the exception of government security services, who are required to produce a court order.[641] At the same time, however, Internet companies

632 Yandex. Privacy Policy. Art. 2.2. https://legal.yandex.ru/confidential.
633 Baidu Statement of Privacy Protection. http://www.baidu.com/duty/yinsiquan.html.
634 Google Privacy Policy. op. cit.
635 Google. About Google Search History. https://support.google.com/accounts/answer/54068?hl=en&ref_topic=14148
636 Yandex. How long are the files stored? FAQ. http://help.yandex.ru/disk/faq.xml#time
637 http://searchengines.guru/showthread.php?t=856569
638 Baidu Statement of Privacy Protection. http://www.baidu.com/duty/yinsiquan.html.
639 Craig Timberg and Jia Lynn Yang. 12 March 2014. Google is encrypting search globally. That's bad for the NSA and China's censors. *Washington Post* The Switch blog. www.washingtonpost.com/blogs/the-switch/wp/2014/03/12/google-is-encrypting-search-worldwide-thats-bad-for-the-nsa-and-china (Accessed 5 May 2014.)
640 Google. Search Help – SSL Search. https://support.google.com/websearch/answer/173733?hl=en
641 Internet companies will be obliged to keep almost all user data. Forbes (Russian) 3 June 2014. http://www.forbes.ru/news/259055-internet-kompanii-obyazhut-khranit-pochti-vse-dannye-o-polzovatelyakh (Accessed 10 July 2014.)

operating in Russia are required to participate in the Law Enforcement Support System, known by its Russian acronym, SORM. Data interception equipment is installed within company facilities. According to Privacy International, the most recently upgraded version of SORM "gathers information from all communication media, and offers long-term storage (three years), providing access to all user data."[642] Thus it is unnecessary for security services to request the information because they may already have direct access to it. If this is not through Yandex directly then it may be via Russian ISPs. At the time of writing, user activity on Yandex.ru was not encrypted.

Among the list of circumstances under which user information might be disclosed **Baidu** includes when "the disclosure is required by laws, regulations, legal proceedings, and government authorities."[643]

Google publishes a transparency report, (to be discussed in more detail in the next section of this case study) that includes global data about "User Data Requests" from governments around the world. From December 31, 2010 to December 31, 2013, the number of requests Google received from governments for user data pertaining to all Google services doubled. The percentage of requests that the company complied with during that same three-year period has steadily declined from 76 per cent to 64 per cent.[644]

4.4.2 Implementation in national context

In the 2014 "Who Has Your Back" report by the US-based Electronic Frontier Foundation (EFF) evaluating U.S. companies on policies and practices related to US government user data requests and surveillance,[645] **Google** was awarded full points in all six possible categories: 1) The company requires a warrant before providing content to U.S. law enforcement; 2) It informs users in the US whenever legally possible before information is disclosed to requesting authorities; 3) It publishes a Transparency Report (see below); 4) It publishes 'law enforcement guides' explaining how the company evaluates and responds to US law enforcement requests; 5) It "fights for user privacy" in the US courts; 6) and it opposes mass surveillance as a member of the Reform Government Surveillance Coalition, which advocates that "governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications."[646]

642 Andrei Soldatov and Irina Borogan. 4 March 2013. Lawful interception: the Russian approach. https://www.privacyinternational.org/blog/lawful-interception-the-russian-approach (Accessed 15 July 2014.)
643 *Baidu Statement of Privacy Protection*, http://www.baidu.com/duty/yinsiquan.html.
644 Requests for User Information. Google Transparency Report. http://www.google.com/transparencyreport/userdatarequests/
645 Who Has Your Back? 2014. Protecting Your Data From Government Requests. Electronic Frontier Foundation. https://www.eff.org/who-has-your-back-2014
646 Reform Government Surveillance. Global Government Surveillance Reform. https://www.reformgovernmentsurveillance.com/

Similar scorecards on Baidu or Yandex have not been produced by civil society or research organizations in their respective home countries. According to the EFF six-point criteria, Yandex would receive one point out of six as the company: it requires a warrant before handing over user data to law enforcement. Yandex has publicly advocated against laws such as the Antipiracy Law that it believes harm freedom of expression online,[647] but there is no publicly available information about the company lobbying in regard to government surveillance practices. Based on information available to this report's researchers, Baidu would score zero out of six. Note that this conclusion does not necessarily reflect the intent of the companies themselves, given that they operate in legal and regulatory environments where a full score is not possible.

4.5 Transparency

Members of the Global Network Initiative, specifically commit to "respect and protect the freedom of expression of their users" in the course of responding to government requests to remove content or hand over user data.[648] They also commit to be held accountable to this commitment. There are two components of public accountability for GNI members: "independent assessment and evaluation" of whether the companies are upholding their commitment to the GNI principles, and also "transparency with the public."[649] Two years after the GNI's official launch with three company members (Google, Microsoft, and Yahoo), the practice of what has come to be called "transparency reporting" began to emerge.

4.5.1 Company practices

In 2010 **Google** was the first Internet company in the world to publish a semi-annual "Transparency Report" including data about the number of government requests that it receives for content restriction as well as the hand-over of user data.[650] Since 2010 the company has also included the percentage of requests it has complied with in each country. In the "Requests to remove content" section, data includes court orders related to cases of defamation brought by individuals.[651] It also includes data about removal or filtering requests received from copyright holders.[652]

---

647 Halia Pavliva. 11 July 2014. Internet Censorship Law Triggers Yandex Tumble. Bloomberg. http://www.bloomberg.com/news/2012-07-11/internet-censorship-law-triggers-yandex-tumble-russia-overnight.html (Accessed 10 August 2014.)

648 Global Network Initiative Principles. Freedom of Expression. http://globalnetworkinitiative.org/principles/index.php#18

649 Global Network Initiative Principles. Governance, Accountability, and Transparency. http://globalnetworkinitiative.org/principles/index.php#22

650 Greater transparency around government requests. Google Official Blog. 20 April 2010. http://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html

651 Requests to Remove Content. From Governments. Google Transparency Report. https://www.google.com/transparencyreport/removals/government/

652 Requests to Remove Content. Due to Copyright. Google Transparency Report. https://www.google.com/transparencyreport/removals/copyright/?hl=en

When search results are removed in response to government or copyright holder demands, a notice describing the number of results removed and the reasons for their removal is displayed to users (see figure 5 below) and a copy of the request to the independent non-profit organization ChillingEffects.org, which archives and publishes the request (see box below for more about the Chilling Effects database).[653] When possible the company also contacts the website's owners.[654]

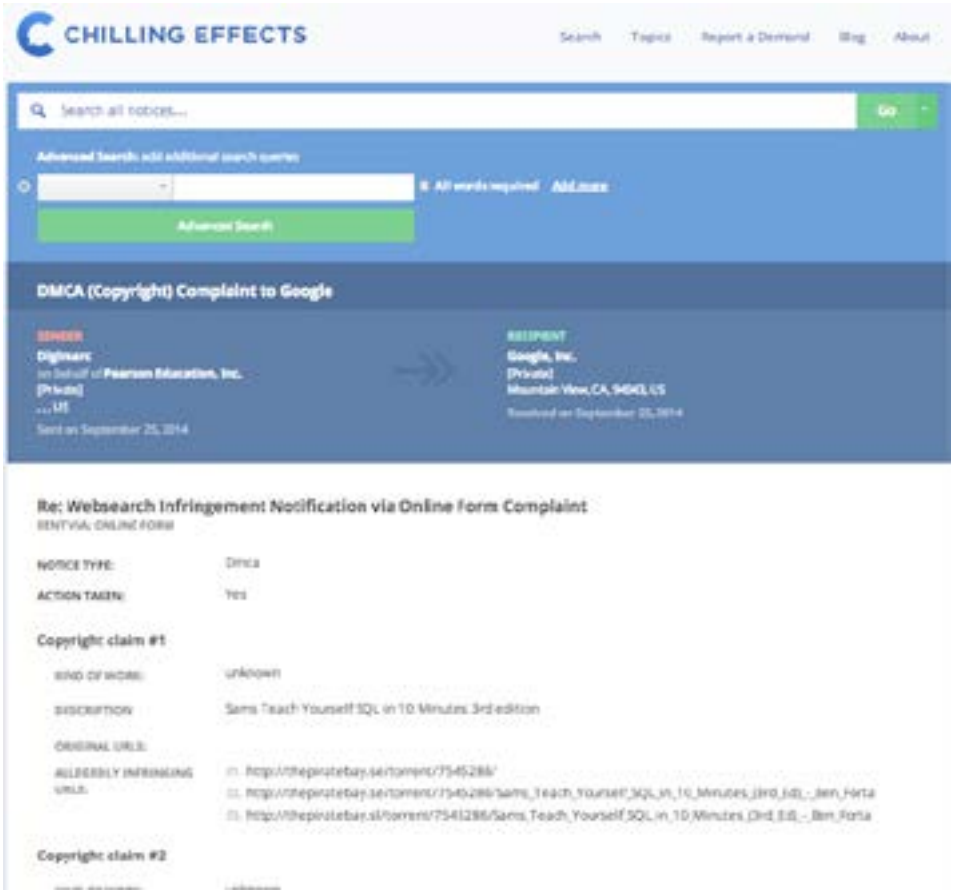
Figure 5: Google notification that content has been removed from search results.

BOX: ChillingEffects.org, a third party clearing house for take-down notices

Founded in 2001, the Chilling Effects database hosted by Harvard's Berkman Center for Internet and Society collects and analyzes legal complaints and requests for removal of online materials. The purpose, according to the project's website, is to help scholars study 'the prevalence of legal threats and let Internet users see the source of content removals.'[655] In 2002, Google started submitting cease-and-desist letters that it received to Chilling Effects. Since then, several other companies including Twittter (see Chapter 5) have chosen to use the project as a neutral third-party host for take-down requests received around the world. The database now includes millions of notices and the project publishes regular analyses of trends in the volume and types of notices received.[656] Below is a screenshot of one copyright notice recently received by Google.

653 DtecNet DMCA (Copyright) Complaint to Google. Chilling Effects Clearinghouse. 12 March 2013. www.chillingeffects.org/notice.cgi?sID=841442.
654 Google. How Google Fights Piracy. September 2013. p.16. https://docs.google.com/a/google.com/file/d/0BwxyRPFduTN2dVFqYml5UENUeUE/edit
655 Chilling Effects. https://www.chillingeffects.org
656 About. Chilling Effects. https://www.chillingeffects.org/pages/about; and for example Huge Volume Increases and Updates to Google Transparency Report. Chilling Effects Blog. 13 December 2012. https://www.chillingeffects.org/blog_entries/585

Figure 6: Example of a take-down notice received by Google and published at Chillingeffects.org[657]



Baidu does notify users about its process for copyright holders to request removal of infringing content.[658] Also, in the case of specific searches containing results that have been removed, Baidu displays a notice at the top of the page announcing: "In accordance with relevant laws and regulations, some search results do not appear."

The company does not publish information about its process for evaluating and responding to government demands. It does not publish data about government requests for content removal or restriction, or about the number of copyright takedown requests received or complied with. The law makes it difficult for Baidu to be more transparent, as Google's experience in China demonstrates. When Google operated its local Google.cn search engine within the jurisdiction of China until early 2010, its transparency report omitted government request data for China. Google explained that data about censorship

657 DMCA (Copyright) Complaint to Google. Digimarc on behalf of Pearson Education, Inc. Chilling Effects. 25 September 2014. https://www.chillingeffects.org/notices/2050759#
658 Baidu. Rights Protection Statement. http://www.baidu.com/duty/right.html

demands are considered state secrets in China and therefore reporting them would be illegal.[659] It would be similarly illegal for Baidu to report data on Chinese government requests. However, it is worth noting that as Baidu expands into other markets outside of China, particularly in Asia,[660] it does not face the same legal barrier to publishing data about requests made by other governments in other jurisdictions.

Yandex does not publish any information about its process for evaluating and responding to government or private demands to remove content. (As mentioned previously, Yandex claims that it does not remove search engine results although it does remove content from other services not covered by this study.) Unlike in China where it would be a violation of law to provide the type of detail found in Google-style "Transparency reports," our researchers were unable to identify any specific Russian law that would prevent Yandex or other Russian Internet companies from publishing statistics about what is being removed, or what volume of requests they receive and what percentage they are complying with. Nor did company representatives explain to our researchers why they do not produce such information, beyond stating that there is no such tradition in Russia.

4.5.2 Transparency in context

India provides an example of how civil society in some countries has begun to use data from Google's transparency report to hold governments accountable for their practices. In 2011, researchers from the Bangalore-based Centre for Internet and Society sent a "right to information" request to the Department of Information Technology (DIT), now the Department of Electronics and Information Technology (DEITY), asking for more information about the number of orders issued by the government for website blocking in India.[661] They then compared the government's responses to the data published in Google's transparency report data on Indian government requests made between January and June 2011, and found that the government had disclosed making substantially fewer requests to Google than Google reported having received from the government. CIS researchers concluded: "Either the DIT is not providing us all the relevant information on blocking, or it is not following the law."[662]

It also appears that lack of transparency can affect public trust in search engines in some countries. In **China**, a lack of transparency about the nature and volume of government restriction requests makes it easier for Chinese users to suspect corruption and foul play. In 2008 Baidu faced widespread accusations in the media and online that it had manipulated search results about the company Sanlu, which had been implicated in a

659 Requests to Remove Content. From Governments. China. Google Transparency Report. https://www.google.com/transparencyreport/removals/government/CN/

660 Asina Pornwasin. Baidu poised for big push into Thailand. 15 October 2013. http://www.nationmultimedia.com/technology/Baidu-poised-for-big-push-into-Thailand-30217048.html (Accessed 25 July 2014.)

661 Text of DIT's Response to Second RTI on Website Blocking. The Centre for Internet & Society. 27 October 2011. http://cis-india.org/internet-governance/dit-response-2nd-rti-blocking

662 Ibid.

scandal over tainted milk powder.[663] Bloggers and members of several online fora accused the company Baidu of burying negative stories about Sanlu at the company's request.[664] Eventually Baidu acknowledged that it had been approached by representatives of the dairy industry offering to pay if the company downplayed certain types of search results, but insisted that it had "flat out refused" to do so.[665]

In 2012 Baidu fired four employees for allegedly taking bribes to remove content from one of its websites after three of the four were arrested.[666] In March 2014, the state-sponsored Beijing News reported that Beijing police had detained "at least 10 people" including Baidu employees for allegedly "abusing their positions to delete online posts in return for money." The article cited "several cases since 2012" in which Beijing police "exposed a profit chain connected to a web censor at the Beijing Municipal Public Security Bureau."[667] One industry source interviewed for this report said, "There are a lot of companies focusing on deleting specific search results," adding, "it's a business now." According to legal experts interviewed for this report, China's courts have dismissed efforts by plaintiffs seeking redress or reinstatement when content that they believed was actually legal was removed for unknown reasons. One interviewee expressed concern that China's online information environment is shaped not only by government officials but also by private sector elites.[668]

4.6 Remedy

There are two potential parties whose freedom of expression rights might be affected by search engines: internet users broadly, and also the creators and operators of websites including individuals with personal blogs and websites, civil society organizations, and news organizations. Other parties can and do have grievances related to other rights – such as content creators concerned about links to file-sharing sites. This section focuses on remedy and grievance mechanisms related only to freedom of expression and not on mechanisms addressing other rights.

---

663 Baidu announcement: Never agreed to block Sanlu negative news. Sina Tech. 13 Sep 2008. http://tech.sina.com.cn/i/2008-09-13/15472456026.shtml.

664 Liu Hongbo: Baidu's brainwash, *Southern Metropolitan News*, 3 May 2010, http://tech.163.com/10/0503/09/65OIDEBF000915BF.html (Accessed 15 April 2014.)

665 Kidney Stone Gate: Baidu Denies Censoring Search Results. ChinaSMACK. 17 September 2008. http://www.chinasmack.com/2008/stories/kidney-stone-gate-baidu-denies-censoring-search-results.html (Accessed 15 April 2014.)

666 Cao Yin. Baidu fires four for deleting posts. China Daily. 8 August 2012. http://usa.chinadaily.com.cn/business/2012-08/08/content_15650874.htm and Baidu Employees Fired and Arrested for Taking Bribes to Delete Content. PCWorld. 6 August 2012. http://www.pcworld.com/article/260498/baidu_employees_fired_and_arrested_for_taking_bribes_to_delete_content.html (Accessed 15 April 2014.)

667 Baidu staff, web censor profited by deleting unfavorable posts. Beijing News. 26 March 2014. http://www.bjd.com.cn/10beijingnews/metro/201403/26/t20140326_6474269.html (Accessed 15 April 2014.)

668 Interviews conducted with sources who wish to remain anonymous; thus date of interviews and identities of interviewees are not disclosed.

None of the search engines studied have complaints, grievance or remedy mechanisms that can be used by internet users who believe that their freedom of expression has been violated due to the way in which a search engine governs its content.

Google does have a mechanism for website owners to challenge removal under the DMCA of links to their websites.[669] Since the company began to implement the European "right to be forgotten" ruling, Google has reinstated links to some news articles that were originally restricted.[670] However the process for handling appeals for reinstatement is not clear. Prior to the roll-out of Google's new "right to be forgotten" web form in the wake of the EU court ruling, none of the search engines studied have provided mechanisms for users to seek remedy if they believe that their privacy rights have been harmed by search results.

While Europeans have successfully used the courts to seek remedy for alleged privacy violations by a search engine, plaintiffs in the countries studied have not been successful in using courts to obtain remedy for search engines' restriction of their websites. Most recently, in 2013 some U.S.-based users of Baidu filed a lawsuit against the company, claiming that Baidu's restriction of content that is not illegal outside of China constituted a violation of their freedom of expression. A United States District Judge dismissed the case against Baidu on the grounds that a search engine's algorithms are protected by the First Amendment.[671]

4.8 Conclusions

This case study has highlighted how search engine policies and practices related to content restriction and content manipulation are shaped by their home jurisdictions, and to varying degrees by the laws and regulations of other jurisdictions. It has also illustrated how three different companies headquartered in three very different national contexts have chosen to handle challenges related to freedom of expression of their users. Key findings include:

Differences in ISP filtering regimes have a strong influence on how, and to what extent, search engines restrict their own search results. For example, due to substantial differences in the technical and legal characteristics of filtering in Russia and China, Yandex and Baidu have very different restriction practices, and Google has taken different approaches to the two markets (remaining in Russia as of August 2014 but removing its operations from China since 2010).

669 Removing Content from Google. https://support.google.com/legal/troubleshooter/1114905?hl=en#ts=1115655,1614942,1727155,1115847

670 Dave Lee. 4 July 2014. Google reinstates 'forgotten' links after pressure. BBC News. http://www.bbc.com/news/technology-28157607 (Accessed 18 July 2014.)

671 U.S. Judge Dismisses Lawsuit Against Chinese Search Engine. Reuters. 28 March 2014. http://www.nytimes.com/2014/03/29/business/us-judge-dismisses-lawsuit-against-chinese-search-engine.html (Accessed 18 July 2014.)

The stricter the liability regime in a given jurisdiction, the more likely the content will be removed either proactively by the company or upon request without challenge. China falls on one end of the spectrum of strict liability and proactive content restriction. But one can also see how the "notice and takedown" system for protecting copyright in the United States can lead to restrictions of legitimate content that a court would likely find it within the search engine's right to display, if the company does not take a strong position in favor of users' rights.

While content restriction takes place on search engines at the request of authorities, it also happens for other reasons in all jurisdictions, including for reasons that the search engines deem to be in the users' or the public's interest. This contradicts a widespread public perception that search engines are neutral arbiters of information. Some consensus among companies and freedom of expression advocates has emerged on best practice by search engines in handling government demands and take down requests from a freedom of expression standpoint, as evidenced by the Global Network Initiative's principles and implementation guidelines. However there is no clear consensus across stakeholders about how search engines should respect freedom of expression in the course of algorithmic design and other content restrictions unrelated to government requests.

Transparency by companies as well as governments plays a crucial role in fostering public trust in a search engine's practices and in ensuring that freedom of expression is not restricted for illegitimate or accidental reasons. The situations discussed in this case study highlight a variety of examples of why it is important that governments be transparent to their citizens about restriction demands being made on search engines as well as the network-level filtering measures that have a direct impact upon them. It is equally important that companies be transparent to users about what is being removed at government or others' request and why.

Privacy concerns are growing but only one of the three companies studied – Google – has addressed these concerns in a public and forthright way. Google has vocally criticized the U.S. government's mass surveillance practices and has been openly lobbying to change them. Neither Baidu nor Yandex have taken similar stands in the face of their governments' surveillance practices. However, many users expect that the companies they rely upon to find information and have their own content found, should be more forthcoming in regard to rights-linked information. This covers as much information about data collection, storage and sharing practices as the law allows, and protecting data to the greatest extent possible within the realities of their legal and political contexts.

Stakeholder engagement, commitment to principles, and remedy frameworks are important for global intermediaries in addressing tensions between freedom of expression and other rights, as well as difficult regulatory situations. Google's commitment to the Global Network Initiative since the organization's launch in 2008, and contribution to the development of the GNI's principles since 2006, has strengthened the company's ability to respect freedom of expression and contest government requests that it and many human rights advocates believe its terms of service are not consistent

with human rights norms. However on other freedom of expression and privacy-related issues not related to government demands, there is no principled framework and no global stakeholder consensus upon which such a framework might eventually be built.

5. STUDY 3: SOCIAL NETWORKING PLATFORMS

Facebook (USA, Germany, India, Brazil, Egypt), Twitter (USA, Kenya) Weibo (China), iWiW. hu (Hungary)

5.1 Introduction

Online social networks play a vital role in social interactions and expression, providing a platform that allows for the democratization of publishing content and information.[672] By enabling the sharing and aggregation of user-generated content, social networks are seen by some to transform 'traditionally passive audiences into active information producers,'[673] providing new tools with the potential for citizens to hold governments accountable.[674]

Social networking companies, like most Internet companies that offer services free of payment, make their profit by targeting advertising to their customers. Third party companies buy advertisements to appear on social networks because they expect these services to be able to identify potential buyers from within their user pool through data collection and processing. Therefore, users 'pay' for the free services they use with their personal information and their privacy. The platforms evolve as their companies develop new ways for users to create and share data.

Social networks have also increased the visibility and reach of some traditional news media, for example, through the 'retweeting' or relaying a microblog to one's connections or the public, thereby disseminating information vastly quicker than conventional means. In China, as one Weibo user pointed out, 'Weibo acts as a source of information and an amplifier. So much has been amplified; so many problems are brought to the public'.[675] A Chinese news service has cited a poll in which 70 per cent of the Chinese public thinks

672 Grabowicz PA, Ramasco JJ, Moro E, Pujol JM, Eguiluz VM. 2012. Social Features of Online Networks: The Strength of Intermediary Ties in Online Social Media. *PLoS ONE*, Vol. 7, No. 1. http://dx.doi.org/10.1371/journal.pone.0029358 (Accessed 10 July 2014.)

673 Yik Chan Chin. August 2013. Regulating social media. Regulating life (and lives). *RJR 33 Online*, p. 4. http://journalism.hkbu.edu.hk/doc/Regulating_social-Media.pdf (Accessed 4 August 2014.)

674 The 2012 Sina Weibo Media Report released on January 2013 by People's Daily Online explained that 'the relatively free atmosphere and the tremendous expression space of Weibo have greatly promoted the openness and transparency of information. Its fission-like communication effect increases the supervision by public opinion . . . Netizens have gained a consciousness of rights, got encouraged to protect their rights by open and legal means.' 2012 *Sina Weibo Media Report*, January 2013, (Accessed 11 August 2014.) http://www.wenming.cn/xwcb_pd/cmcy/201301/P020130123314840012552.pdf.

675 Weibo Opinion Leaders' Observation of China. 25 November 2010. *Time Weekly*. www.time-weekly.com/story/2010-11-25/421.html. (Accessed 11 August 2014.)

that online expression 'will become a new avenue for China's democratic development'.[676] A representative from an Egyptian NGO has noted that, as people use social media 'to call for marches or protests, and other political events . . . they [become] an outlet for the people to express their impressions and what is on their minds'.[677]

Many legal systems consider social networks as 'content hosts', because users create content on their platforms, and third parties are allowed to post and share information.[678] Because they allow private content to be publicly shared, social networks blur the line separating the public and private spheres, raising questions about appropriate expectations for expression on such platforms – i.e. should expression on Facebook be treated the same as expression in a news article or a blog?[679]

Due to the scope and impact of user-generated expression and activity on social networks it is not easy for a company to balance a commitment to free expression, legal compliance, and user expectations as well as the fiduciary duty as companies to make profits.[680] This study examines the policies and practices of several social networking platforms in a range of national contexts. It finds that the ability of social networking platforms to respect users' freedom of expression is heavily influenced by national legal and regulatory contexts, particularly by the context of a company's home country. At the same time, the cases analyzed clearly show that companies have many options available to them in terms of how they manage and design their platforms. These choices have a critical impact on users' freedom of expression.

The Companies Studied:

Facebook (www.facebook.com). Facebook is a US-based social network founded in 2004. As of March 2014, the company had 1.28 billion monthly active users– of which 81.2 per cent were located outside of North America.[681] It allows registered users to maintain a personal profile through which users can share personal and contact information, photos, articles and location statuses; to communicate with other users via private or public messages; to search and 'friend' other users, whom they may 'tag' in photos or location updates; and to join groups and interact with other members. Facebook is available on the world wide web as well as through dedicated applications on a number

676 China's Sina Weibo microblog nears identity deadline. 12 March 2012. *BBC News*. www.bbc.com/news/technology-17337252 (Accessed 11 August 2014.)

677 Emad Mubarak, Executive Director, Association for Freedom of Thought and Expression. Interview with Sara Alsherif. Cairo, Egypt, 22 April, 2014.

678 Internet intermediaries: Dilemma of Liability. *Article 19*. 2013. p. 6. http://www.article19.org/data/files/Intermediaries_ENGLISH.pdf

679 Tarleton Gillespie. 2010. The Politics of 'Platforms'. *New Media & Society*, Vol. 12, No. 3, pp. 347–64. http://dx.doi.org/10.1177/1461444809342738 (Accessed 4 August 2014.) The legislative strategy of platforms (here: YouTube) as a middle way of being 'rewarded for facilitating expression but not liable for its excesses' (p. 356); on the one hand highlighting the crucial role of their services for 'unfettered circulation of information', for some other reasons downplaying their role as 'merely in intermediary, to limit its liability for the users' activity' (p. 356).

680 Sean Rintel. 5 January 2014. A thin blue line: how Facebook deals with controversial content. http://theconversation.com/a-thin-blue-line-how-facebook-deals-with-controversial-content-19966 (Accessed 24 June 2014.)

681 Facebook. Newsroom – Statistics. http://newsroom.fb.com/company-info

of mobile operating systems.[682] For this study, Facebook's operations were examined in Brazil, Egypt, Germany, India and the United States.

Twitter (www.twitter.com) Twitter is a US-based micro-blogging platform founded in 2006. As of June 2014, it had 271million monthly active users who send 500 million messages (called 'Tweets') a day. Seventy-seven per cent of Twitter's users live outside of the United States.[683] Twitter allows registered users to exchange messages of 140 (or fewer) characters through the Twitter website, mobile application(s) or SMS. Users can forward such messages by 'retweeting' them. Users can also search for and 'follow' other users, and even unregistered people can read users' Tweets, as long as the users have kept their profile public (the default setting).[684] Twitter is accessible on the world wide web and via multiple mobile applications. Tweets can be organized via hashtags (the hash sign # followed by a word or phrase), allowing users to group related posts together. If a hashtag receives high volumes of 'retweets' it is termed to be 'trending'.[685] Twitter does not 'require real name use, email verification, or identity authentication'.[686] Twitter was studied primarily in the United States and Kenya.

Weibo (www.weibo.com) Weibo, is a Chinese micro-blogging platform founded in 2009 that was spun off from Sina, its original parent company, prior to its public listing of shares in the United States in April 2014.[687] As of June 2014 it boasted 156 million monthly active users.[688] Users have personal profiles, post 140-character messages (called **weibo**, which literally means 'microblog' in Chinese) and comment under other **weibo**, a key feature that provides a 'simple way for Chinese people and organizations to publicly express themselves in real time'.[689] For this report, Weibo was studied in China.

iWiW (formerly www.iwiw.hu) iWiW ('international who is who') is a now-defunct Hungarian social network that closed operations in July 2014 due to its diminishing user base.[690] It was founded in April 2002 as wiw.hu ('who is who'),[691] and became iWiW in October 2005, when it unsuccessfully tried to expand and began offering its platform in multiple

682 For more information about Facebook products, see Facebook. Newsroom – Products. http://newsroom.fb.com/products
683 Twitter. About Twitter. https://about.twitter.com/company
684 Twitter. Help Center. About public and protected Tweets. https://support.twitter.com/articles/14016-about-public-and-protected-tweets (Accessed 28 July 2014.)
685 About Twitter op. cit.
686 Twitter. Guidelines for Law Enforcement. https://support.twitter.com/articles/41949-guidelines-for-law-enforcement#5
687 Sina Corporation. About Sina. http://corp.sina.com.cn/eng/sina_intr_eng.htm. Kaylene Hong. 28 March 2014. China's Twitter' Sina Weibo drops 'Sina' from its name as it prepares to list in the US. *The Next Web*. http://thenextweb.com/asia/2014/03/28/chinas-twitter-sina-weibo-drops-sina-from-its-name-as-it-prepares-to-list-in-the-us (Accessed 10 August 2014.)
688 Xinhua08.com. 15 August 2014. Weibo Monthly Active Users Exceed 156 million [in Chinese]. http://news.xinhua08.com/a/20140815/1371610.shtml (Accessed 10 August 2014.)
689 Weibo Corporation. November 2014. Form 6-K to the United States Securities and Exchange Commission. Posted at http://ir.weibo.com/phoenix.zhtml?c=253076&p=irol-sec
690 iWiW, The Hungarian Social Network Closes After 12 Years of Success. 19 May 2014. *Daily News Hungary*. http://dailynewshungary.com/iwiw-the-hungarian-social-network-closes-after-12-years-of-success (Accessed 25 June 2014.)
691 Anikó Imre. May 2009. National intimacy and post-socialist networking. *European Journal of Cultural Studies*, Vol. 12, No. 2, pp. 219–33. http://dx.doi.org/10.1177/1367549409102428 (Accessed 25 June 2014.)

languages.[692] In April 2006 it was acquired by T-Online, Magyar Telekom's business unit,[693] and in 2008 iWiW merged with Origo.hu.[694] Until 2011 it was invitation-only.[695] In January 2013 it had 4.7 million registered users.[696] For this report, iWiW was studied in Hungary.

Social networks are popular around the world but they are used differently in different cultural and political contexts.[697] Facebook and Twitter are two of the most popular social networks with broad international user bases, and thus a study of these services can shed light on freedom of expression issues in a transnational environment. iWiW and Weibo are primarily domestic operations. Weibo is especially interesting because the Chinse social-media market is highly competitive yet insulated from foreign competition.[698] iWiW was chosen for this study (prior to being closed down) because it represents a domestic social networking service trying to compete in a local linguistic and cultural context against global competitors.

5.2 Impact of ISP filtering on social networking platforms

As discussed in Chapter 3, governments can require ISPs to filter social networking platforms by blocking access either to the entire website, or to specific content, groups or pages. Such filtering can also take place at national internet exchange points as described in the previous case studies.

Facebook, Twitter and YouTube (owned by Google) are reported by local internet users to have been consistently filtered in China for a long period of time, rendering them completely inaccessible to Chinese internet users unless special circumvention technology is used.[699] (For a full discussion and definition of network-level filtering, please see Study 1.) Other countries, including Iran, Pakistan and Turkey, have also filtered these social networking platforms for varying periods of time.[700]

---

692 Adam Straub. 14 April 2012. Miért nem az iWiW lett a Facebook? [Why not have a Facebook iWiW?]. Origo. (In Hungarian.) www.origo.hu/techbazis/20120412-tizeves-az-iwiw-interju-varady-zsolttal-a-kozossegi-szajt.html (Accessed 8 August 2014.)

693 Magyar Telekom. 28 April 2006. T-Online gains control of iWiW. www.telekom.hu/static/sw/download/WIW28April_eng.pdf (Accessed 5 August 2014.)

694 Borbála Tóth. 5 January 2012. Mapping Digital Media: Hungary. Open Society Foundations. p. 42. www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-hungary-20120216.pdf

695 Blase Ur and Yang Wang. Online social networks in a Post-Soviet state: How Hungarians protect and share on Facebook. Paper presented at iConference '12, February 7–10, Toronto (Canada). 2012. http://www.blaseur.com/papers/ur_wang_iconference12_hungary.pdf.

696 Unsocial network: the rise and fall of iWiW. *Budapest Business Journal*. 7 January 2013. www.bbj.hu/business/unsocial-network-the-rise-and-fall-of-iwiw_64418 (Accessed 6 April 2014); Átlépte a 4 milliót az iWiW felhasználók száma! [iWiW crosses the 4 million number!]. PenzCentrum.hu. (In Hungarian.) www.penzcentrum.hu/vasarlas/atlepte_a_4_milliot_az_iwiw_felhasznalok_szama.1015273.html

697 Pew Global. Social Networking popular across globe. *Pew Research Global Attitutes Project*. 12 December 2012. http://www.pewglobal.org/2012/12/12/social-networking-popular-across-globe/ (Accessed 28 July 2014.)

698 Loretta Chao and Josh Chin. China Eases Crackdown on Internet. op.cit.

699 Freedom House. Freedom on the Net 2013. China www.freedomhouse.org/report/freedom-net/2013/china

700 Dana Liebelson. 28 March 2014. MAP: Here Are the Countries That Block Facebook, Twitter, and YouTube. *Mother Jones*. www.motherjones.com/politics/2014/03/turkey-facebook-youtube-twitter-blocked (Accessed 7 August 2014.)

Companies that operate social networking platforms have no control over actions by governments and ISPs to filter them. Some have spoken out against network-level filtering in general, as Facebook, Twitter, and Google have done.[701] However, companies do exercise control over their terms of service and also respond to government requests to remove content or deactivate accounts on their own platforms. Companies' decisions about such platform-level restrictions may in turn affect whether or not governments choose to filter at the network level.

Governments restrict social networks via network-level filtering under several circumstances:

Differences in norms of the jurisdictions: Unlike ISPs, social networks – as well as search engines discussed in the previous case study - do not require a physical presence in a country in order to reach users in it. However some governments use the threat of network level filtering in an effort to compel companies to comply with their laws.

For example, in 2011 the Delhi High Court asked Facebook (along with Google) to 'develop a mechanism to monitor and remove offensive and objectionable material' and threatened to filter them 'like China' if they did not comply.[702] As previously mentioned in Study 1, in 2013, a Brazilian judge ordered Facebook to remove content about a fight between two neighbours and threatened to block Facebook if it refused. The judge reportedly viewed the company's intransigence as an insult to Brazil's sovereignty. Facebook did not comply and the threat was not carried out.[703]

To prevent political unrest and preserve national unity: From July 2009-May 2010, the Chinese government implemented a network shutdown in the northwestern province of Xinjiang in response to unrest.[704] Since then, Facebook and Twitter have been filtered nationwide and cannot be accessed without the use of special circumvention technology.

In 2011, the Egyptian government filtered Facebook and Twitter, prior to shutting down internet access across the country for approximately one week. In this instance, filtering of Facebook and Twitter was not permanent and inconsistently implemented as access was intermittently available when internet service itself was available.[705]

---

701 For example, Facebook and Twitter spoke out against the internet ban that took place in Egypt in 2011. For more information see: Google, Facebook and Twitter speak out against Egypt's Internet ban. AFP via France24. 2 February 2011. http://www.france24.com/en/20110202-google-facebook-twitter-egypt-internet-ban-mubarak/ (Accessed 5 August 2014.)

702 Facebook and Google remove 'offensive' India content. 6 February 2012. BBC. www.bbc.com/news/world-asia-india-16903765 (Accessed 5 August 2014.)

703 Rafael Sabarai. 3 October 2013. *Briga de Vizinho pode tirar Facebook do ar no Brasil*. [Neighbor fights can take air in Brazil Facebook]. *Veja*. http://veja.abril.com.br/noticia/vida-digital/acao-judicial-pode-deixar-facebook-fora-do-ar-no-brasil (Accessed 8 April 2014.)

704 Edward Wong. 15 May 2010. After Long Ban, Western China Is Back Online. *New York Times*. www.nytimes.com/2010/05/15/world/asia/15china.html (Accessed 5 August 2014.)

705 Confusion over Egyptian blocks on web protest tools. 26 January 2011. *BBC News*. accessed 13 July 2014, www.bbc.co.uk/news/technology-12291982; At a glance. Twitter. 1 January 2011 – 28 February 2011. *Herdict.* http://www.herdict.org/explore/indepth;jsessionid=92376A04145A81FEAED45F53F0858298#!fs=2633&fc=EG&fed=02/28/2011&fsd=01/01/2011 (Accessed 13 July 2014); At a glance. Facebook. 1 January 2011 – 28 February 2011. *Herdict.* http://www.herdict.org/explore/indepth;jsessionid=92376A04145A81FEAED45F53F0858298#!fs=2633&fc=EG&fed=02/28/2011&fl=&fs=2245&fsd=01/01/2011 (Accessed 13 July 2014.)

Real-time need to control to and maintain public order: Governments issue orders for the network-level filtering of social networking platforms when there is a perceived need to maintain public order. One example cited in Study 1 occurred in India in 2012 when the government, responding to threats of ethnic and sectarian violence following unrest in the northeast, ordered ISPs to filter pages on YouTube, Facebook and Twitter that featured inflammatory content and requested that the companies remove content and block accounts).[706]

5.3 Content removal and account deactivation

While social networking platforms can be the target of ISP-level filtering over which they have no direct control as described above, social networks do have their own mechanisms to block or otherwise restrict user content. This section discusses such mechanisms and the different contexts in which they are deployed.

Social networking platforms generally require users to create an account – i.e. a username and password – in order to share content. Operators of the platforms can restrict content that users share on the platform in several ways: deleting content; blocking it from view for users in specific jurisdictions; or shutting down – deactivating - the accounts of users who post certain content. These actions may be taken as a self-regulatory measure to enforce private rules, or in compliance with government requests and other legal requirements such as responding to court orders in civil cases. The table below provides an overview of the different modes through which these actions occur, reasons, and affected parties.

Table 3: Key factors affecting content restriction by social networking platforms:

Reason for restriction:	Content violates terms of service?	Modes of implementation:	Who is affected:
• government requests • law-based requests (e.g. copyright takedown notices, court orders in civil cases) • self-regulation on own initiative (terms of service and other enforcement of private rules) • user reporting (on other users' violations of terms of service)	• possibly • possibly • Usually • Usually	• complete removal of specific content • blocking of specific content for a specific user group or jurisdiction (content remains accessible to others) • automated (pro-active) filtering of pre-identified types of content	• all users • only users in a particular jurisdiction • only specific user groups (for example by age)

706 Vikas SN. 22 August 2012. #IndiaBlocks: Airtel Blocks Youtu.be Short URL, Proxy & Domain Marketplace Sites. *MediaNama*. www.medianama.com/2012/08/223-indiablocks-airtel-blocks-youtu-be-short-url-proxy-domain-marketplace-sites (Accessed 4 August 2014.)

The next two sub-sections will examine company policies related to these different modes of restriction, as well as their implementation in the context of jurisdictions covered by this case study.

5.3.1 Government requests and legal requirements

Company Policies

Facebook and Twitter, with large user bases outside their home jurisdictions, may act to restrict content in response to lawful requests from governments.

Child sexual abuse images are the only type of illegal content that Facebook and Twitter pro-actively monitor and remove without first having received a government request, court order, or copyright takedown notice. In 2011, Facebook was the first company to employ Microsoft's PhotoDNA, which can identify known child sexual abuse photos 99.7 per cent of the time.[707] Twitter has used it since 2013.[708]

Both companies publicly explain their policies for responding to all other restriction requests from authorized authorities in their home jurisdiction and around the world.[709] In cases where the content in question does not violate the companies' terms of service and is not illegal in the United States, Facebook and Twitter may use a jurisdiction-specific restriction mechanism: content is restricted only to users in jurisdictions where it found to be infringing according to local law and where governments have made specific lawful requests.[710] This way, content remains accessible to users outside the jurisdiction where the law compels its restriction.

Weibo does not have a public policy dedicated to content restriction requests from authorized authorities, but a leaked Sina internal document appeared to highlight a direct 'backdoor' access to Weibo's servers, which reportedly allows officials to filter keywords

---

707 Riva Richmond. 19 May 2011. Facebook's New Way to Combat Child Pornography. *New York Times*. http://gadgetwise.blogs.nytimes.com/2011/05/19/facebook-to-combat-child-porn-using-microsofts-technology (Accessed 5 August 2014); Nick Eaton. 19 May 2011. Facebook deploys Microsoft tool to fight child pornography. *Seattle Post-Intelligencer*. http://blog.seattlepi.com/microsoft/2011/05/19/facebook-deploys-microsoft-tool-to-fight-child-pornography (Accessed 5 August 2014); Bill Harmon. 19 May 2011. 500 million friends against child exploitation. The Official Microsoft Blog. http://blogs.microsoft.com/blog/2011/05/19/500-million-friends-against-child-exploitation (Accessed 5 August 2014.)

708 Charles Arthur. 22 July 2013. Twitter to introduce PhotoDNA system to block child abuse images. *The Guardian*. www.theguardian.com/technology/2013/jul/22/twitter-photodna-child-abuse (Accessed 5 August 2014.)

709 Twitter. Guidelines for law enforcement. https://support.twitter.com/groups/56-policies-violations/topics/238-report-a-violation/articles/41949-guidelines-for-law-enforcement#11 Facebook. Safety Center. Information for Law Enforcement Authorities. https://www.facebook.com/safety/groups/law/guidelines

710 Facebook restricts content on a reactive basis and on receipt of requests from governments, law enforcement and nongovernmental organizations. Facebook. Government requests report. FAQs. https://govtrequests.facebook.com/faq/ and Facebook. Government requests report. About the report. https://govtrequests.facebook.com/about Twitter restricts content on a reactive basis and on receipt of 'a valid and properly scoped request from an authorized entity'. Twitter. Help Center. Country Withheld Content. https://support.twitter.com/articles/20169222-country-withheld-content

and delete content without having to go through the company.[711] iWiW did not have publicly available guidelines on dealing with governmental requests to restrict content, and was not available for comment.

Implementation in national context

All of the social networking platforms studied in this research are affected by law in their home jurisdiction as well as by law in other countries where they actively market their service to users. It is important to note however that governments have less leverage over social networking services that do not have offices or employees physically located in their jurisdiction. Laws related to intermediary liability (see Chapter 2) in the home jurisdiction, as well as in other jurisdictions where the platforms have high commercial interest, appear to have particularly strong influence on how companies shape their content restriction policies and practices.

In cases where a social networking platform is completely filtered at the network level for a long period of time in a given jurisdiction, the company must decide whether or not to concede to that country's legal requirements in order to possibly get the filter removed and thus restoring restore access to that market.[712] In the case of China, neither Facebook nor Twitter has made that concession.[713]

China's 'blanket liability' regime for intermediaries means that social networking platforms are responsible for all content – even that which is user-generated and which the company is not aware of. SinaWeibo seems the only company studied in this research that is known to proactively monitor user content (other than child abuse images), because it needs to comply with Chinese law and the demands of regulators. In China's strict regulatory environment, there is no public evidence of Weibo contesting government requests for content restriction. Details of Weibo's implementation will be discussed later in this section.

There is no evidence of iWiW having challenged government requests in Hungary, but this may be because the government had not issued takedown requests; there is insufficient public information available to know for sure.

The US-based Facebook and Twitter are broadly exempt from liability for third-party content under US law – Section 230 of the CDA (see Chapter 2) – which specifically

711 Sophie Beach. 11 March 2013. Beyond censors' reach, free expression thrives, to a point. Challenged in China: The shifting dynamics of censorship and control. *Committee to Protect Journalists*. https://www.cpj.org/reports/2013/03/challenged-china-media-censorship-weibo-expression.php (Accessed 10 August 2014.)

712 Gibran Ashraf. Two years on, no light at the end of the tunnel for YouTube. 18 September 2014. *The Express Tribune.* http://tribune.com.pk/story/763869/two-years-on-no-light-at-the-end-of-the-tunnel-for-youtube/ (Accessed 3 October 2014.)

713 Censors in China keep mainlanders in dark about Hong Kong protests. 29 September 2014. *The Los Angeles Times.* http://www.latimes.com/world/asia/la-fg-censors-in-china-keep-mainlanders-in-dark-about-hong-kong-protests-20140929-story.html (Accessed 3 October 2014.)

maintains that intermediaries do not have to monitor user content.[714] This serves as the baseline for the companies' policies related to government requests and other legal compliance requirements at home and around the world.

Intermediaries do receive many copyright-related takedown requests in accordance with copyright laws. Because Facebook and Twitter are headquartered in the United States they delete content globally in compliance with DMCA takedown requests. (see Chapter 2 for a discussion of the DMCA). Facebook and Twitter have different mechanisms to receive these requests.[715] (The Transparency and Remedy sections of this case study will describe how users are notified of requests and takedowns, as well mechanisms for appeal.)

Practices of Facebook and Twitter in context:

As will be discussed in greater detail later in the 'Transparency' section of this case study, of the social networking platforms studied, only Facebook and Twitter publish information about the volume and type of requests received by governments as part of what the industry has come to call 'transparency reports'. Their data show that requests and companies' compliance rates vary widely from country to country – and also between companies – thus shedding light not only on different legal regimes but also illuminating some basic characteristics of these companies' policies and practices in relation to government requests.

The following table lists the number of items restricted by Facebook in response to government requests (but not court orders in civil cases or copyright takedowns) between July-December 2013 in all jurisdictions covered by all three case studies in this report. It also includes some basic information about the reason for restriction as disclosed by the company. (Countries where no requests were made are omitted.)

714 Roxanne E. Christ, Jeanne S. Berges and Shannon C. Trevino. July 2007. Social Networking Sites: To Monitor or Not to Monitor Users and Their Content? *Intellectual Property and Technology Law Journal*, Vol. 19, No. 7, p. 2. www.lw.com/thoughtLeadership/social-networking-monitoring-content-texas-case

715 See 17 U.S.C. § 512 (i)(1)(A). Legal Information Institute. www.law.cornell.edu/uscode/text/17/512 (Accessed 11 August 2014); James Gibson. 12 July 2011. The DMCA and Repeat Infringers. The Media Institute. www.mediainstitute.org/IPI/2011/071211.php (Accessed 11 August 2014.)

Table 4: Facebook content restricted at government request, July-December 2013[716]

Brazil	0*	"We restricted content in Brazil in response to requests related to defamation and orders in civil cases. We have not reported defamation or civil claims in this report. We may include these sorts of requests in future reports."
Germany	84	"We restricted access in Germany to a number of pieces of content reported under local laws prohibiting Holocaust denial."
India	4,765	"…reported primarily by law enforcement officials and the India Computer Emergency Response Team under local laws prohibiting criticism of a religion or the state."
Russia	4	"We restricted access in Russia to a number of pieces of content reported by the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications under local laws prohibiting access to certain forms of drug-use and self-harm."
UK	3	"We restricted access to content in the UK in response to a small number of court injunctions."

The next table contains Twitter's similar but more detailed breakdown of restrictions made in response to government requests and court orders during the same time period, in jurisdictions covered by this report. (Countries where no requests were made are omitted.)

Table 5: Twitter content restricted at government request July-December 2013[717]

Country	Removal requests - Court Orders	Removal requests - Gov't agency, police, other	Percentage where some content withheld	Accounts specified	Accounts withheld	Tweets withheld
Brazil	11	1	33%	50	2	26
Germany	1	1	0%	<10	0	0
India	2	6	13%	54	0	13
Russia	0	14	64%	14	1	9
UK	1	8	0%	<10	0	0
USA	2	6	0%	11	0	0

Because Facebook does not publish data about the number of requests versus the number honored, it is not clear how Facebook's compliance rate may or may not differ from Twitter's. Twitter for its part does not shed light on the reasons for requests or what type of subject matter they relate to. The nature of the services is also sufficiently different that a direct comparison may have limited meaning. Nonetheless these numbers help to shed some light (even if still murky) on how companies respond to government requests

716 Facebook. Government Requests Report. https://govtrequests.facebook.com/
717 Twitter Transparency Report. Removal Requests. July 1 – December 31, 2013. https://transparency.twitter.com/removal-requests/2013/jul-dec

differently in different jurisdictions – and which governments tend to make the most requests.

Twitter's data shows that, in the countries covered by this report, the company chose not to comply with a large percentage of government restriction requests it received in the second half of 2013. This indicates that, in a substantial number of cases, Twitter apparently determined that either a) the request itself was not in full compliance with the law where the request was made; b) its lawyers determined that the content was not infringing in that jurisdiction, or c) that the company otherwise had a legal right in that particular context to decline.

During the same reporting period, Twitter received the highest number of requests from Brazil and Russia. Facebook also restricted some content in Russia for the same period in compliance with "local laws prohibiting access to certain forms of drug-use and self-harm." Twitter specifies that most of its requests from Brazil came as court orders. Facebook clarifies that while it received no government agency requests in Brazil for that period, it did restrict content in Brazil due to defamation and orders in civil cases, even though the company did not provide data on those restrictions.

Another significant data point is the high number of restrictions Facebook carried out at the request of the Indian government - 4,765. This is by far the highest number of restrictions Facebook carried out in any jurisdiction. The high number reflects the legal and regulatory environment of India, discussed in Chapter 2, in which intermediaries have considerable liability for user content and government has the legal authority to require removal of broad categories of content. The company nonetheless makes an effort to limit such restrictions so that the content remains visible in other jurisdictions where it is not illegal. For example, in 2012 Facebook complied with a court order and restricted 'objectionable' material cited as causing communal unrest in India, but maintained public visibility for the content when viewed from IP addresses not located in India.[718]

Both Twitter and Facebook restrict content in Germany. In its first implementations of its 'Country Withheld Content policy' in 2012, Twitter blocked access to the account of a white supremacist organization to users in Germany, upon request from German law enforcement.[719] In that case, because the user's entire account was targeted for restriction by authorized authorities in a single country, Twitter did not delete the account, but instead restricted access to the account for German users only.[720] Twitter is the only

718 Note: this order was from the Delhi High Court that targeted Facebook, Yahoo, Orkut and 21 other internet companies for hosting 'objectionable' content. For more information see: BBC, Facebook and Google remove 'offensive' India content. 6 February 2012. BBC. www.bbc.com/news/world-asia-india-16903765 (Accessed 5 August 2014.)

719 Twitter Transparency Report. Removal requests. July 1 – December 31, 2012. https://transparency.twitter.com/removal-requests/2012/jul-dec

720 Freedom House Foundation (ed.). Freedom on the Net Report - Germany 2013. http://www.freedomhouse.org/report/freedom-net/2013/germany; Kate Connolly. 18 October 2012. Twitter blocks neo-Nazi account in Germany. *The Guardian*. www.theguardian.com/technology/2012/oct/18/twitter-block-neo-nazi-account (Accessed 4 August 2014.)

company in this study that reports account restrictions (as opposed to content restriction) due to government requests.[721]

Figure 7: Screenshot of the blocked account of a German far-right group when accessed from a German IP address.[722]

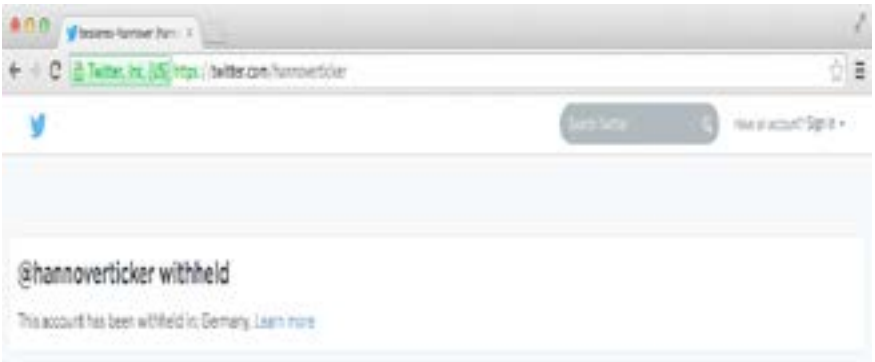


Figure 8: Screenshot of the same account accessed from a US IP address. The account holders stopped using it after it was blocked in Germany.[723]

Even with jurisdictional blocking, companies do not accept all requests. In March 2014, a Brazilian court ordered Facebook to delete the Page of Eduardo Campos, a presidential candidate in the 2014 elections. As of this writing the page is still accessible in Brazil.[724]

721 Twitter Transparency Report. Information requests. July 1 – December 31, 2013. https://transparency.twitter.com/information-requests/2013/jul-dec; Twitter Transparency Report. Information requests. January 1 – June 30, 2013. https://transparency.twitter.com/removal-requests/2013/jan-jun

722 Screenshot 22 July 2014. https://twitter.com/hannoverticker

723 Screenshot 22 July 2014. https://twitter.com/hannoverticker

724 Correio Popular. 5 March 2014. TSE manda retirar site 'Eduardo Campos Presidente'. http://correio.rac.com.br/_conteudo/2014/03/capa/nacional/158198-tse-manda-retirar-site-eduardo-campos-presidente.html (Accessed 8 April 2014). Yet as of date the page is still accessible on Facebook - See page on facebook https://www.facebook.com/groups/eduardocampospresidente/?ref=br_tf.

BOX: jurisdictional blocking in other countries

There are a few other prominent examples from outside of the case study countries worth mentioning, as they help highlight other key dimensions to jurisdictional blocking. In France, Twitter blocked specific Tweets containing the hashtags #UnBonJuif ('a good Jew') and #UnJuifMort ('a dead Jew'), upon request of a French Jewish student group. Twitter explained, 'Based on local law, we withheld access to some, but not all, of the reported Tweets in France'.[725] In Turkey, Twitter acknowledged problematic aspects of having to comply with local law to block content locally when it complied with a request to block an account that accused a former Turkish government minister of corruption.[726] This move happened at the same time that Twitter was temporarily blocked in Turkey after Twitter users had posted information accusing government figures of corruption.[727] Civil society advocacy groups have criticized Twitter for too easily using jurisdictional blocking. It temporarily blocked 'blasphemous' content in Pakistan and a right-wing Ukrainian group's Twitter account in Russia.[728] Twitter denied Russian assertions that it had blocked further accounts alleged to be extremist.[729]

As will be discussed further in section 5.3.2, Facebook and Twitter also remove content and deactivate accounts to enforce their own terms of service, separate from what the law requires. Both companies have mechanisms through which any individual can flag a piece of content or user account for violating Facebook's Community Standards and Twitter's equivalent, called 'The Twitter rules'.

Industry sources confirmed to this report's researchers that authorities of some governments sometimes also seek to have content restricted via the companies' own self-regulatory mechanisms, rather than make formal requests through official channels following legally specified process. As of this writing, neither company has included in its transparency reports any data about the extent to which governments in various countries use the companies' own self-regulatory mechanisms designed for individuals to report content that violates the terms of service. (Notably, Google's transparency report does include information about content that governments have sought to have removed from

725 Twitter removes French anti-Semitic Tweets. *BBC News*. 19 October 2012. http://www.bbc.com/news/technology-20004671 (Accessed 16 July 2014.); François Delerue. The French Twitter Case: A Difficult Equilibrium between Freedom of Expression. *Digital Evidence and Electronic Signature Law Review*. vol. 10 (November 2013) pp. 193-197. http://sas-space.sas.ac.uk/5444/1/2042-2947-1-SM.pdf.

726 Vijaya Gadde. 26 March 2014. Challenging the access ban in Turkey Wednesday. *Twitter Blog*. https://blog.twitter.com/2014/challenging-the-access-ban-in-turkey (Accessed 8 August 2014); Sam Schechner and Ayla Albayrak. 26 March 2014. Twitter Keeps Up Turkey Fight but Blocks an Account. *Wall Street Journal. Digits*. http://blogs.wsj.com/digits/2014/03/26/twitter-keeps-up-turkey-fight-but-blocks-an-account (Accessed 8 August 2014.)

727 Officials in Turkey 'lift Twitter ban. *BBC News*. 3 April 2014. http://www.bbc.com/news/world-europe-26873603 (Accessed 16 July 2014.)

728 Robert Mackey. 18 June 2014. Twitter Restores Access to 'Blasphemous' Tweets in Pakistan. *New York Times*. http://news.blogs.nytimes.com/2014/06/18/twitter-restores-access-to-blasphemous-tweets-in-pakistan (Accessed 4 July 2014); Activists fight Twitter censorship in Pakistan with #TwitterTheocracy. 11 June 2014. *Al Jazeera*. http://stream.aljazeera.com/story/201406111324-0023825 (Accessed 28 July 2014.)

729 Robert Mackey. 18 June 2014. Twitter Restores Access to 'Blasphemous' Tweets in Pakistan. *New York Times*. http://news.blogs.nytimes.com/2014/06/18/twitter-restores-access-to-blasphemous-tweets-in-pakistan (Accessed 4 July 2014); Ilya Khrennikov and Sarah Frier. 24 June 2014. Twitter Denies Blocking Extremist Accounts in Russia. *Bloomberg*. www.bloomberg.com/news/2014-06-23/russia-says-twitter-to-block-extremists-such-as-ukraine-group.html (Accessed 16 July 2014.)

its video sharing service, YouTube, and which the company agreed to remove because it violated the platform's terms. However YouTube was not covered in this study.)

Practices of Weibo in context:

China is the only country in this case study that requires intermediaries to proactively monitor user content. In China, if too much of the information users share on social media platforms falls into the 'nine forbidden content categories' (see Chapter 2), the company can have its operating licenses revoked.[730] Failure to comply satisfactorily with government requirements can have serious consequences: during an anti-pornography crackdown in April 2014 the government revoked Sina's publishing and media distribution licenses.[731] As such Weibo's terms of service – as with all internet intermediaries in China – closely mirror the legal requirements imposed by the Chinese government and Weibo proactively monitors and deletes content in order to retain its operating licenses.[732]

According to a Carnegie Mellon study of Weibo, about 16 per cent of all messages are deleted.[733] Reuters has reported that within an average 24 hour period Weibo's staff must process and make decisions about three million Weibo posts.[734] The *China Digital Times,* a project housed at the University of California Berkeley, has a long-term project to track Weibo's list of sensitive words. Researchers have found that the addition of new words and terms into the company's list of sensitive words appeared to be correlated with political and social events. Researchers also found that the list apparently also contained a large number of homophones and similar expressions in order to limit access to information about particular controversies. For instance, in January 2014, 'Xi', Chinese

730 Article 35, *Measures on the Administration of Internet Information Services* (Deliberation Draft). 7 June 2012. sina.com. http://news.sina.com.cn/c/2012-06-07/135924552816.shtml (Accessed 16 July 2014.)

731 Michael Martina. 25 April 2014. Sina shares fall after China strips its licence in web porn crackdown. *Reuters*. www.reuters.com/article/2014/04/24/china-internet-sina-idUSL3N0NG4EG20140424 (Accessed 4 August 2014.) –are there no other sources for this but Western?

732 Since the second half of year 2011, China Digital Times has been running an independent test aiming at the keywords that are blocked in Sina Weibo search and publish the test results from time to time. On October 17 of the same year, the project started to collect clues from the public and named itself as the open-source project of sensitive words in Sina Weibo's search. This project now publishes a open list of banned words in Sina Weibo's search, which records more than one thousand words and expressions that were or are blocked. See http://chinadigitaltimes.net/chinese/%E6%96%B0%E6%B5%AA%E5%BE%AE%E5%8D%9A%E6%90%9C%E7%B4%A2%E6%95%8F%E6%84%9F%E8%AF%8D%E5%88%97%E8%A1%A8/.

733 David Bamman, Brendan O'Connor and Noah Smith. March 2012. Censorship and deletion practices in Chinese social media. *First Monday*, Vol. 17, No. 3. http://dx.doi.org/10.5210/fm.v17i3.3943 (Accessed 5 August 2014); Allen Yu. 23 March 2012. Carnegie Mellon Study on Censorship and Deletion Practices in Chinese Social Media. Stanford Law School Center for Internet and Society Blog. http://cyberlaw.stanford.edu/blog/2012/03/carnegie-mellon-study-censorship-and-deletion-practices-chinese-social-media (Accessed 5 August 2014.)

734 Li Hui and Megha Rajagopalan. 11 September 2013. At Sina Weibo's censorship hub, China's Little Brothers cleanse online chatter. Reuters. http://www.reuters.com/article/2013/09/12/us-china-internet-idUSBRE98A18Z20130912 (Accessed 12 September 2014.)

President Xi Jinping's surname, Xi, appeared to have been filtered when it was combined with expressions such as 'publicity stunt', 'sensationalism' and 'playacting'.[735]

Chinese social networking platforms use a variety of other methods to comply with government censorship requirements. Keyword blocking is the most popular. Weibo maintains a blacklist of keywords that users are unable to use in their posts. For example the screenshot below illustrates a case in which the user attempted to post an item mentioning the "New Citizen Movement." A message appeared stating: 'Sorry, this post is not suitable for public display'.

In other instances, terms might trigger a program that flags the post it for editorial review before it can be published. In some cases, censors can leave the post visible to the author but block its visibility to others, thus not alerting users to the fact that a post is being restricted.[736]

Terms or user names can also be blocked from appearing in the platform's search function, for instance, a search for a the name of the artist Ai Weiwei, is met with a message that says: 'In accordance with relevant laws and regulations, the search results for "Ai Weiwei" do not appear'.

Sometimes specific features can be temporarily disabled: In March 2012 authorities reportedly instructed Sina Weibo to disable commenting – its liveliest and most popular feature – for three days.[737] Chinese authorities and social networking platform operators can be extremely specific about the granularity of some restrictions. This granularity can be geographic; for example, after the July 2012 Beijing floods, Beijing-based Weibo users searching for 'Beijing' reported to see only users whose handles included the word 'Beijing' – but no posts *about* the floods.[738]

Despite the heavy restrictions, some argue that Weibo remains an outlet for controversial expression even if for short periods of time. One employee pointed out that news *does* often get out in the several minutes before something is deleted.[739]

---

735 This project now publishes an open list of banned words in Weibo's search, which records more than one thousand words and expressions that were or are blocked. For test results, refer to this continuously updated document "新浪微博搜索敏感词列表（更新中）Sensitive Sina Weibo Search Terms (Updating)", *Google Docs,* accessed 16 July 2014, https://docs.google.com/spreadsheet/ccc?key=0Aqe87wrWj9w_dFpJWjZoM19BNkFfV2JrWS1pMEtYcEE#gid=0.

736 Li Hui and Megha Rajagopalan. At Sina Weibo's censorship hub, China's Little Brothers cleanse online chatter. op. cit.; Sina Weibo Community Management Regulations (Trial). *Sina Weibo.* 8 May 2012. http://chinacopyrightandmedia.wordpress.com/2012/05/08/sina-weibo-community-management-regulations-trial (Accessed 7 August 2014.)

737 Loretta Chao and Josh Chin. 2 April 2012. China Eases Crackdown on Internet. op. cit.

738 Coincidence? Sina Weibo's Curious Breakdown. 27 July 2012. *Wall Street Journal* China Real Time Blog. http://blogs.wsj.com/chinarealtime/2012/07/27/coincidence-sina-weibos-curious-breakdown (Accessed 11 August 2014.)

739 Interviewee agreed to be held on condition of anonymity. Threfore name, time and location of interview have been withheld.

5.3.2 Company Self-regulation

Companies reserve the right to restrict content from the platform that violates their terms of service.[740] All social networking platforms prohibit some content in their terms of service[741] or easier-to-understand guidelines like the 'Facebook Community Standards'[742] or 'The Twitter Rules'.[743] In addition to prohibiting content that is illegal in their home jurisdictions, many restrict access to content that may be legally protected speech (especially in the US) but which the company has chosen to disallow: Such content generally includes categories such as adult pornography, nudity, hate speech, harassment, impersonation, and private information like someone's credit card or government ID number.[744] Facebook users with 'Pages' (as opposed to personal profiles) have the option to filter common profanity or self-selected words.[745] iWiW, for example, prohibits usernames that contain a public figure's name.[746]

Account restrictions

All companies reserve the right to revoke certain privileges, suspend or terminate user accounts at their discretion without prior notice.[747] This can happen in response to any of the reporting mechanisms described below. However, some Facebook and Twitter policies hint that summary account terminations are rare; Twitter explains it 'will make reasonable efforts to notify you' by email or the next time users log in.[748] Weibo may warn the user or summarily suspend or terminate the account.[749]

In countries where laws restrict broad categories of speech, companies' terms of service reflect the legal regime. Weibo's 'Community Convention Administrative Regulations' prohibits content that criticizes the government.[750]

---

740 https://twitter.com/tos, Sina Weibo – http://service.account.weibo.com/roles/guiding. , iWiW - http://iwiw.hu/i/felhasznalasi-feltetele

741 Facebook Terms https://www.facebook.com/legal/terms; Twitter terms of service. https://twitter.com/tos; Sina Weibo Community Management Regulations. http://service.account.weibo.com/roles/guiding (for translation see http://chinacopyrightandmedia.wordpress.com/2012/05/08/sina-weibo-community-management-regulations-trial/) ; iWiW Tems of Service. http://iwiw.hu/i/felhasznalasi-feltetele

742 Facebook. Community Standards. https://www.facebook.com/communitystandards

743 Facebook's Statement of Rights and Responsibilities: 'You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.' Twitter. The Twitter Rules. https://support.twitter.com/articles/18311-the-twitter-rules

744 The Twitter Rules: 'You may not use our service for any unlawful purposes or in furtherance of illegal activities. International users agree to comply with all local laws regarding online conduct and acceptable content.'

745 Facebook. Desktop Help. How can I proactively moderate content posted on my Page? https://www.facebook.com/help/131671940241729.

746 iWiW terms of service, *Felhasználási Feltételek*. http://iwiw.hu/i/felhasznalasi-feltetelek

747 iWiW reserves the right to, at the company's discretion, terminate and remove content for a number of additional reasons. For more information see: terms of service. Felhasználási Feltételek. http://iwiw.hu/i/felhasznalasi-feltetelek; https://support.twitter.com/articles/18311-the-twitter-rules; Facebook Terms, op. cit.

748 Twitter terms of service op. cit.

749 *Sina Weibo Community Management Regulations* (trial). http://service.account.weibo.com/roles/guiding; Li Hui and Megha Rajagopalan. op. cit.

750 Sina Weibo Community Regulations. op. cit.

Most social networking platforms including those covered by this research have automated mechanisms to detect spam.[751] However, sometimes these computer programs unsupervised by humans can make mistakes when the user's actions or the content of their postings display patterns common to spam. For example in 2012, a journalist's comment on Facebook was mistakenly flagged as spam.[752] On Twitter, spam can must be reported by a user clicking on a Tweet from the alleged spammer's profile.

Reporting mechanisms

Companies allow people to report either content or individual users that are abusive, or that otherwise violates terms of service. The companies evaluate these reports and have an internal process for deciding whether and how to take action if warranted.

Facebook offers forms to users, as well as to those who do not have an account, to report different types of violations including abuse, nudity, and the potential spreading of private information.[753] Facebook specifies that reported content is reviewed manually, and if the content in question violates the company's 'Community Standards', it will remove it from the platform for all jurisdictions.[754] Facebook has outsourced much of the process of manually reviewing reported content,[755] although sources knowledgeable about Facebook's operations have said that the outsourced company sends difficult cases back to Facebook staff for further review.[756] Users who report a violation can track how their report is being handled through a Support Dashboard.[757] Facebook also uses a 'social reporting' mechanism that allows users to reach out to trusted friends to help them resolve issues. For example, when one user posts unflattering or false information or pictures about another, the subject can make a direct removal request to the person who

751 Facebook. Desktop Help. Spam.https://www.facebook.com/help/287137088110949; Twitter. Help Center . Reporting spam on Twitter. https://support.twitter.com/articles/64986-reporting-spam-on-twitter.

752 Christina DesMarais. 6 May 2012. Facebook Spam Filter Catches Some By Surprise. *TechHive*. www.techhive.com/article/255101/facebook_and_spam_not_everything_is_relevant.html (Accessed 29 July 2014); Emil Protalinski. 5 May 2012. Facebook blames Scoble snafu on spam false positive. *ZDNet*. www.zdnet.com/blog/facebook/facebook-blames-scoble-snafu-on-spam-false-positive/12589.

753 Facebook. Desktop Help. Report a Violation. https://www.facebook.com/help/263149623790594.

754 Sean Rintel. A thin blue line: how Facebook deals with controversial content. 5 January 2014. http://theconversation.com/a-thin-blue-line-how-facebook-deals-with-controversial-content-19966 (Accessed 16 July 2014); Facebook. What Happens After You Click 'Report'. 19 June 2012. https://www.facebook.com/notes/facebook-safety/what-happens-after-you-click-report/432670926753695.

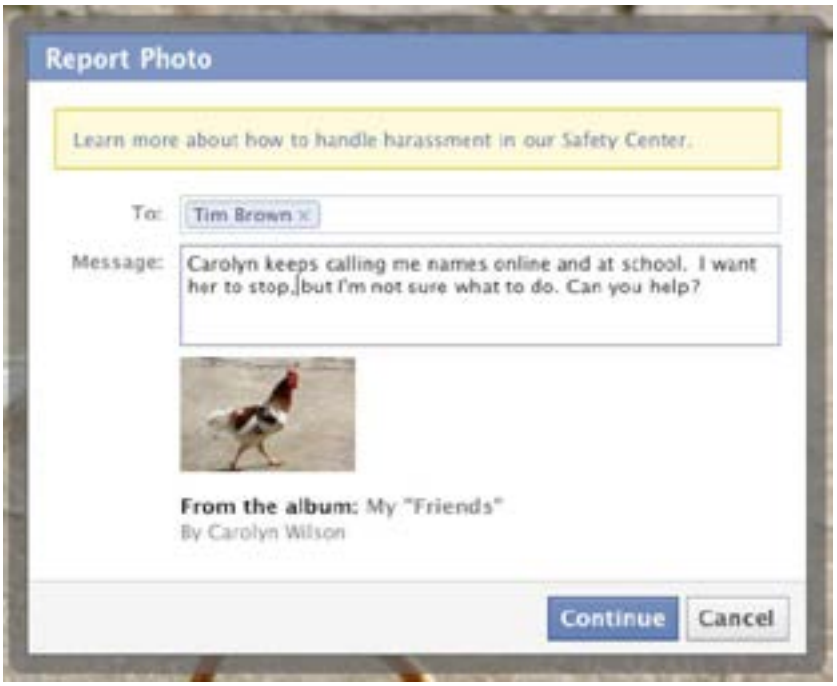
755 Note: in the past this role was outsourced to a company called oDesk as reported in the source in this footnote. According to an industry source speaking on condition of non-attribution, Facebook no longer works with oDesk although it is known to work with another other company performing the same function. Details about any new outsourcing arrangements are not publicly available. Adrian Chen. Inside Facebook's Outsourced Anti-Porn and Gore Brigade, Where 'Camel Toes' are More Offensive Than 'Crushed Heads. *Gawker.* 16 February 2012, http://gawker.com/5885836/facebook-releases-new-content-guidelines-now-allows-bodily-fluids.

756 Details of interview omitted on the requests of the interviewees.

757 Facebook. More Transparency in Reporting. 26 April 2012, https://www.facebook.com/notes/facebook-safety/more-transparency-in-reporting/397890383565083.

posted the content. Or one user can use a special form to reach out to a friend requesting help in countering harassment by a third user:[758]

Figure 9: Example of a Facebook form seeking a friend's help in countering harassment, as provided by the company to users



Reporting mechanisms can be useful in addressing abusive behaviour and content, but oftentimes people misuse the reporting mechanism merely to report content that they do not like. Facebook has been accused of removing activists' pages for reasons that were not clear to the creators of the page.[759] Facebook claims that 'number of times something is reported doesn't determine whether or not it's removed',[760] but some activist groups have alleged that mass abuse reporting by apparent government agents in some countries has led to content removal.[761]

758 Facebook. Details on Social Reporting. 10 March 2011. https://www.facebook.com/notes/facebook-safety/details-on-social-reporting/196124227075034

759 Shiv Malik. 29 April 2011. Facebook accused of removing activists' pages. *The Guardian*. http://www.theguardian.com/technology/2011/apr/29/facebook-accused-removing-activists-pages (Accessed 10 August 2014.)

760 Facebook. About Facebook's Security & Warnings Systems. https://www.facebook.com/help/408181689281891 (Accessed 10 August 2014.)

761 Vietnam Blocks Dissident Facebook Pages Through Fake Abuse Reports. 21 July 2014. *Radio Free Asia*. www.rfa.org/english/news/vietnam/facebook-07212014182948.html (Accessed 4 August 2014)

Twitter has also has mechanisms allowing users to report content via web forms.[762] It details how to report the various violations on one web page titled "how to report violations'.[763] One may report Tweets and Twitter account holders for impersonation, trademarks, harassment, and self-harm. Users can also 'report an ad': Twitter advertisements are not allowed to promote 'illegal products, services, or content'.[764] Some advertisements are restricted by geography: In Brazil the company prohibits any advertising related to political campaigning.[765] Below is an image of the reporting mechanism for advertisements:

Figure 11: Twitter's form to report advertisements that violate the company's rules

Similarly, **Weibo** has a reporting mechanism through which users can report posts, comments and private messages that they believe are abusive or infringing of company policy. Weibo users are encouraged to use the 'report abuse' function for 'false information', especially if it concerns natural disasters, and information that may have been exaggerated to gain attention.[766]

Prior to its closure, **iWiW** also had online forms for reporting abuse.[767]

Company enforcement

Companies explain how they enforce their rules for user behavior and acceptable content to varying degrees. Some companies provide very specific examples, whereas others use imprecise language that allows companies to exercise discretion.

762 Twitter Help Center. How to report violations. https://support.twitter.com/articles/15789
763 Twitter. How to report violations. https://support.twitter.com/groups/56-policies-violations/topics/238-report-a-violation/articles/15789-how-to-report-violations
764 Twitter. Help Center. Twitter Ads Policies. https://support.twitter.com/articles/20169693-twitter-ads-policies
765 Twitter. Advertiser policies: Political campaigning. https://support.twitter.com/articles/20170492
766 Sina Corp. Help Center: Report Abuse. http://help.sina.com.cn/comquestiondetail/view/1045
767 Deutsche Telekom AG. Implementation Questionnaire. Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU. *ICT Coalition*. 11 October 2013. p. 11-12. http://www.ictcoalition.eu/gallery/ICT%20Principles_Compliance%20Report%20Deutsche%20Telekom%20Group%20080114-08012014021423.pdf.

Facebook can mete out tiered punishments; e.g. if someone sends repeatedly sends spam, Facebook may block just the messaging features for that user.[768] It does commit to notifying users the next time they log in.[769] **Twitter** posts a clear notification that an account has been suspended – even for users who are merely trying to view the suspended account. The below screenshot taken in August 2014 is an example:

When an account is found to violate the company's terms, it is removed globally from the platform. For example, in the wake of the 2013 Westgate Mall terror attack in Kenya, Twitter suspended a number of accounts belonging to a Somali militant group for spreading content that was abusive and violent in nature.[770] In this case, the decision to suspend the accounts was based on a determination that they violated Twitter's own rules. Such cases do not appear in Twitter's transparency reports because the company only publishes data about content removals that are made in response to formal government requests or court orders. In other words, the company does not publish data about content removed for violating its 'Twitter rules' – presumably, even if that content was brought to the company's attention by a government authority using the company's self-regulatory mechanism for reporting 'Twitter rules' violations.

In 2007, **iWiW** deleted the profile of Magyar Gárda, a Hungarian right-wing paramilitary group, because it violated iWiW's rule that only allows natural persons – i.e. no organizations – to create accounts. It also received hundreds of user complaints about the profile's 'propagandistic nature', which also violated its terms.[771] Gárda supporters alleged cried 'double standards', pointing to the 'many political organisations' on iWiW, including 'the openly communist Munkáspárt [Hungarian Workers' Party]'.[772]

768 Facebook Desktop Help. Why does Facebook limit the use of certain features and what are the limits?
https://www.facebook.com/help/177066345680802

769 Facebook. Statement of Rights and Responsibilities. https://www.facebook.com/legal/terms

770 Bernard Oginga. 22 September 2013. Al Shabaab twitter acount shut down after Kenyan attack. *Standard Digital*. www.standardmedia.co.ke/?articleID=2000094048&story_title=al-shabaab-twitter-account-shut (Accessed 7 April 2014); Hamza Mohamed. Al-Shabab in long-running battle with Twitter. Aljazeera. 18 Dec 2013, http://www.aljazeera.com/indepth/features/2013/12/al-shabab-long-running-battle-with-twitter-201312171127155596 8.html (Accessed 7 April 2014.)

771 See Magyar Gárda profile deleted by iWiW. Népszabadság Online 28 august 2007 (Törölte az iWiW a Magyar Gárda adatlapját). [translation]. (In Hungarian.) http://nol.hu/archivum/archiv-462071-265440; Magyar Gárda deleted from iWiW. Index. 28 August 2007 (Törölték a Magyar Gárdát az iWiW-ről), available at: http://index.hu/bulvar/iwiwgarda372/; Magyar Gárda kicked off, Fodor Gábor allowed to stay on iWiW Heti Válasz. 28 August 2007. http://hetivalasz.hu/migr_lt_cikk_gy_ujtu/a-magyar-garda-ropult-fodor-gabor-viszont-maradhatott-az-iwiw-en-16827/?cikk_ertekel=1&ertekeles=3 (Accessed 10 August 2014.)

772 The Hungarian Guard (Magyar Gárda) has been object of cenzorship on iwiw.hu. Ex-homár Blog. 28 August 2007. http://ex-homar.blogspot.com/2007/08/hungarian-guard-magyar-grda-has-been.html (Accessed 10 August 2014.)

In 2012 **Weibo** enacted 'Community Management Regulations' announcing that users would be recruited to form a committee[773] that votes on how to deal with reported content.[774] Weibo deletes accounts belonging to the worst violators of its content rules, which aligns closely with laws and government requirements.[775] Weibo's account deletions have spawned 'reincarnation parties' where participants create hundreds of new accounts.[776] However reincarnation can be thwarted: Journalist Yang Haipeng's Weibo account appeared to have been closed in April 2012, and while he reported repeated attempts to reopen it under a variety of coded user names, in each of the 65 attempts, accounts were ultimately closed.[777] The artist Ai Weiwei also resported that he was repeatedly unable to register, possibly due to blocks associated with his IP addresses or ID numbers now required for registration.[778]

Violations of company terms of service are unevenly enforced. Furthermore, Facebook and Twitter have been known to reverse their decisions after receiving negative publicity for their handling of specific cases. For example, a German TV host received a notification stating that his post criticizing the Catholic Church's stance on same-sex marriage violated community guidelines.[779] As a public figure, he was able to draw attention to Facebook's arbitrariness. Facebook apologized for the 'mistake'.780

Conversely, content is sometimes found to violate the company's rules and deleted only after activists or the media call attention to it. For example, Facebook deleted the big-game hunting photos of 19-year-old Kendall Jones after environmental activist groups expressed outrage. Facebook said that they violated its terms of service as 'graphic

773 Sina Weibo Community Management Regulations (Trial). Unofficial translation published at China Copyright and Media. 8 May 2012. http://chinacopyrightandmedia.wordpress.com/2012/05/08/sina-weibo-community-management-regulations-trial (Accessed 5 August 2014.)

774 Sina Weibo Community Convention (trial). http://service.account.weibo.com/roles/gongyue; Sina Weibo Community Management Regulations (trial). http://service.account.weibo.com/roles/guiding; and Sina Weibo Community Committee System (trial). http://service.account.weibo.com/roles/zhidu.

775 Li Hui and Megha Rajagopalan. At Sina Weibo's censorship hub, China's Little Brothers cleanse online chatter. op. cit.

776 Bei Feng. 26 November 2012. Microblogs Have Become the Focus of Internet Censorship in China. Human Rights in China. www.hrichina.org/en/crf/article/6406 (Accessed 1 August 2014.)

777 Sophie Beach. 11 March 2013. Beyond censors' reach, free expression thrives, to a point. Challenged in China: The shifting dynamics of censorship and control. *Committee to Protect Journalists*. https://www.cpj.org/reports/2013/03/challenged-china-media-censorship-weibo-expression.php (Accessed 10 August 2014.)

778 Sui-lee Wee. 19 March 2012. Ai Weiwei says censors removed his microblog. *Reuters*. www.reuters.com/article/2012/03/19/us-china-artist-microblog-idUSBRE82I09U20120319 (Accessed 10 August 2014.)

779 Jürgen Domian. No title. *Facebook*, 18 March 2013. www.facebook.com/Domian.Juergen/posts/466265690110405 (Accessed 19 June 2014.)

780 Tina Kulow. 19 March 2013. *Was ist mit dem Post von Domian passiert*? [What has happened to the post of Jürgen Domian?]. Public Official Facebook Statement. (In German.) https://de-de.facebook.com/notes/tina-kulow/was-ist-mit-dem-post-von-domian-passiert/625428644149658. (Accessed 19 June 2014.)

images shared for sadistic effect or to celebrate or glorify violence'.[781] In May 2013, Facebook temporarily banned certain violent videos, and then quietly reversed its decision in July. A video of a woman being beheaded by members of an organized crime cartel in Mexico only entered public consciousness when BBC wrote about it in October. Facebook first declined to remove the video, but later reversed its position due to public and political pressure.[782]

Both Facebook and Twitter have in recent years grown more transparent about how they repond to government requests for content restriction made through formal legal channels or other official, legally binding processes. However as several examples in this section and the previous section show, both companies are much more opaque about their internal decision-making processes around how and when their own rules are enforced.

5.4 Privacy

Social networks are veritable treasure troves of private information, revealing everything from political preferences to sexual orientation. Users implicitly entrust social networks with personal data. Governments for their part make requests for private user information in the pursuit of civil, criminal, and even national security investigations.

5.4.1 Company policies

All companies examined in this case study have privacy policies of some form that explain how user information is used, but the policies are rarely straightforward or comprehensive.

Weibo does not have a privacy policy per se but several provisions of its Community Regulations address privacy;[783] its parent, Sina, also has a privacy statement. The statement discusses the personally identifiable information that the company collects and provides individuals the option to opt out of receiving information from the company.[784]

781 Chris Taylor. 7 July 2014. Facebook: Here's Why We Deleted Cheerleader's Hunting Pics. *Mashable*. http://mashable.com/2014/07/07/facebook-kendall-jones (Accessed 11 August 2014); Charlotte Allen. In defense of Texas huntress and conservationist Kendall Jones. *Los Angeles Times*. 16 July 2014. www.latimes.com/opinion/opinion-la/la-ol-kendall-jones-texas-hunter-cheerleader-20140716-story.html (Accessed 11 August 2014); Molly Wharton. 9 July 2014. Hunting Photos Glorify Violence, but 'Kill Kendall Jones' Facebook Page Apparently Doesn't. *National Review Online*. www.nationalreview.com/corner/382355/hunting-photos-glorify-violence-kill-kendall-jones-facebook-page-apparently-doesnt (Accessed 11 August 2014.)

782 Will Grant. 3 November 2013. Facebook beheading video: Who was Mexico's Jane Doe? *BBC News Magazine*. www.bbc.com/news/magazine-24772724 (Accessed 11 August 2014.)

783 Sina Weibo terms of service http://service.account.weibo.com/roles/guiding (Accessible only after login.)

784 Sina Corp. About Sina: Privacy. http://corp.sina.com.cn/chn/sina_priv.html

Facebook decided to call its privacy policy a 'Data Use Policy' (DUP) in a September 2011 update.[785] Facebook is unique in this study in promising users a seven-day period to comment on proposed changes to its DUP on the dedicated 'Site Governance Page'.[786]

Twitter's Privacy Policy explains that when 'material' changes to the policy are made, users will receive a @Twitter update or email.[787]

iWiW's privacy policy provided notice to users of changes to the policy. Users accept the modifications of the privacy policies by logging into the service after the modifications had entered entry into force.[788]

Data Retention

Companies studied do not offer much information about data retention. **Weibo** does not provide any information. **Facebook** is vague: it stores data 'for as long as it is necessary to provide products and services to you and others' – typically 'until your account is deleted'.[789] **Twitter** explains that 'log data' – i.e. metadata – is deleted or anonymized after 18 months at the latest.[790] **iWiW** stated that data was retained for as long as the user is a member, with user content like status updates and photos 'displayed' to the user's contacts for 14 days and stored at most for 21 days, while metadata is stored for six days.[791]

Disclosure of User Data

Facebook and **Twitter** have policies that describe how they respond to government requests for user data. Facebook and Twitter, unless legally restricted, notify the user if an authorized authority requested user account information.[792]

Weibo's parent Sina states that it may be required by law to disclose personal information under several circumstances: (1) compliance with legal notices or applicable legal

---

785 Laurie Segall. 23 March 2012. Facebook strips 'privacy' from new 'data use' policy explainer. *CNN Money*. http://money.cnn.com/2012/03/22/technology/facebook-privacy-changes (Accessed 9 August 2014); Facebook. Data Use Policy. Last updated 15 November 2013. https://www.facebook.com/full_data_use_policy (Accessed 9 August 2014.)

786 Facebook. Data Use Policy: Some other things you need to know. https://www.facebook.com/about/privacy/other

787 Twitter Privacy Policy. https://twitter.com/privacy

788

789 Facebook. Information we receive and how it is used. https://www.facebook.com/about/privacy/your-info.

790 'We receive Log Data when you interact with our Services, for example, when you visit our websites, sign into our Services, interact with our email notifications, use your Twitter account to authenticate to a third-party website or application, or visit a third-party website that includes a Twitter button or widget. Twitter uses Log Data to provide our Services and to measure, customize, and improve them. If not already done earlier, for example, as provided below for Widget Data, we will either delete Log Data or remove any common account identifiers, such as your username, full IP address, or email address, after 18 months.' Twitter Privacy Policy. last updated 21 October 2013. https://twitter.com/privacy (Accessed 4 August 2014.)

791 iWiW Privacy Policy. *Adatkezelési szabályzat*. http://iwiw.hu/i/adatkezelesi-szabalyzat , art. 9A, 9E, 9F.

792 Twitter. Help Center. Guidelines for Law Enforcement. https://support.twitter.com/entries/41949; Facebook. Safety Center. Information for Law Enforcement Authorities. https://www.facebook.com/safety/groups/law/guidelines

procedures; (2) protection of the rights or property of users; (3) In an emergency situation, in order to protect personal or public safety.[793]

iWiW did not describe in any detail how it responded to government and other lawful requests for user data. The company did mention in its privacy policy that it did not need user consent in instances of data transfer mandated by law, and gave no mention of any procedure for notifying users after the transfer had taken place.[794]

Real-name requirements

The UN Special Rapportueur for Freedom of Expression and the UN High Commissioner for Human Rights have both flagged the importance of anonymity, as linked to the right to privacy, for the exercise and protection of human rights in the internet age. Many social networking platforms, but not all, require that users sign up with their real names and inforce such policies to varying degrees and in a variety of ways.

Twitter is the only company examined without a real-name policy; it only asks for an email at registration. Facebook, iWiW and Weibo require real names for various reasons. Chinese law compels Weibo to verify identities.[795] iWiW required that users register with their genuine first and last names and reserved the right to ask users to verify personal information.

Facebook states that a real name policy 'leads to greater accountability and a safer and more trusted environment'.[796] It has enforced this policy with varying degrees of effort and consistency over time. The deactivation of prominent pseudonymous accounts has made media waves, especially when the accounts of celebrities including the author Salman Rushdie were deleted. As of August 2014, Facebook stated that it allows persistent pseudonyms (e.g. Snoop Dogg) but uses an algorithm to verify what it deems patently false names.[797] Furthermore, people who want to change their names are required to submit proof of identification.[798]

793 Sina Corp. About Sina: Privacy. http://corp.sina.com.cn/chn/sina_priv.html
794 iWiW Privacy Policy. *Adatkezelési szabályzat*. http://iwiw.hu/i/adatkezelesi-szabalyzat , art. 8H.
795 XinhuaNet. February 10, 2012. 'Four questions' about Weibo real name policy (original source: People's Daily Overseas Edition) [in Chinese]. http://news.xinhuanet.com/society/2012-02/10/c_111507519.htm (Accessed 9 August 2014.)
796 Somini Sengupta. 15 November 2011. Rushdie Wins Facebook Fight Over Identity. *New York Times*. www.nytimes.com/2011/11/15/technology/hiding-or-using-your-name-online-and-who-decides.html?pagewanted=all (Accessed 9 August 2014.)
797 Facebook. Desktop Help – Get Started on Facebook – Signing Up. My name was rejected during signup. https://www.facebook.com/help/212848065405122
798 Facebook. Desktop Help: Changing Your Name. www.facebook.com/help/contact/245617802141709

Although Facebook promises to 'permanently delete your ID from [its] servers' after confirming that you are indeed using your real name,[799] there is no way for the user to verify this. One mitigating factor is that users may submit two IDs of lesser value – e.g. bus cards, magazine subscription stubs, yearbook photos – instead of driver's licenses or passports.[800]

Account settings

Default settings have significant privacy ramifications because human beings are subject to 'default bias'.[801] As regulatory scholar Cass Sunstein put it, 'defaults are powerful influences of choice, even when the stakes are high'.[802]

Although it is primarily a public-facing network, **Twitter** does allow users to tweet privately to a select group of followers (protected Tweets cannot be retweeted, nor can they show up in searches).[803] Accounts on Twitter and Weibo are set to public by default.

Facebook has experimented with default settings. At the time of writing, users had the option to choose whether to share content publicly, to their 'networks' or only to friends.

799 Facebook. Desktop Help: What happens to my ID after I upload it? https://www.facebook.com/help/155050237914643

800 Facebook. Desktop Help: What types of ID do you accept? https://www.facebook.com/help/159096464162185

801 Cass Sunstein. December 2013. Deciding by Default. *University of Pennsylvania Law Review*, Vol. 162, No. 1. p. 14. http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1000&context=penn_law_review

802 Eric J. Johnson, Steven Bellman and Gerald L. Lohse. 2002. Defaults, Framing, and Privacy: Why Opting In–Opting Out. *Marketing Letters*, Vol. 13, No. 1. pp. 13–14. https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf

803 Twitter Help Center. About Public And Protected Tweets. https://support.twitter.com/articles/14016-about-public-and-protected-tweets

In December 2009, Facebook changed the default setting to 'public', while announcing in a press release that granular privacy options heralded a 'new standard in user control'.[804] In May 2014, however, Facebook changed the default setting for new users back to 'sharing with friends'.[805]

Facebook users' names, gender, profile pictures, background ('cover') photos and networks are always visible to everyone.[806] On iWiW, name, nickname, country, town and gender were always public.[807] Pictures were visible to friends of friends.[808] Also, users were required to choose a location from a drop-down menu at registration, though this was not verified and could easily be changed.[809]

Facebook, iWiW and Weibo allow users to choose whether search engines can index their accounts; all public Twitter accounts are open to be indexed.[810] Weibo users are not given the option to make their account visible only to confirmed followers, but users can disable comments and block specific users.[811]

5.4.2 Implementation in national context

The following section examines the outcomes produced by specific company policies and practices relating to data collection, retention, and sharing with third parties, in the context of particular regulatory and legal environments.

Data protection and privacy enforcement

Facebook has faced legal action over 'deceptive' privacy policies. In 2011, the US Federal Trade Commission (FTC) fined Facebook for first telling users they could keep

804 Facebook Asks More Than 350 Million Users Around the World To Personalize Their Privacy. *Facebook Newsroom*. 9 December 2009. http://newsroom.fb.com/news/2009/12/facebook-asks-more-than-350-million-users-around-the-world-to-personalize-their-privacy (Accessed 8 August 2014); Ryan Singel. 9 December 2009. Public Posting Now the Default on Facebook. *Wired*. www.wired.com/2009/12/facebook-privacy-update (Accessed 8 August 2014.)

805 Making It Easier to Share With Who You Want. *Facebook Newsroom*. 22 May 2014. http://newsroom.fb.com/news/2014/05/making-it-easier-to-share-with-who-you-want (Accessed 8 August 2014);

806 Facebook. Desktop Help. What's considered public information? https://www.facebook.com/help/167709519956542

807 Blase Ur and Yang Wang. Online social networks in a Post-Soviet state. op. cit.; iWiW Privacy Policy, *Adatkezelési szabályzat*, available at http://iwiw.hu/i/adatkezelesi-szabalyzat, art. 7a, 7c, 7d.

808 iWiW Privacy Policy, Adatkezelési szabályzat, available at http://iwiw.hu/i/adatkezelesi-szabalyzat, art. 7d; iWiW terms of service, Felhasználási Feltételek, available at http://iwiw.hu/i/felhasznalasi-feltetelek.

809 Balázs Lengyel, Attila Varga, Bence Ságvári and Ákos Jakobi. 26 January 2013. Distance dead or alive Online Social Networks from a geography perspective. SSRN. http://dx.doi.org/10.2139/ssrn.2207352

810 Facebook Desktop Help. Appearing in Search Engine Results. https://www.facebook.com/help/392235220834308; Privacy policy of Origo Média és Kommunikációs Szolgáltató Zrt., operator of iWiW.hu community website. *iWiW, Adatkezelési szabályzat*. http://iwiw.hu/i/adatkezelesi-szabalyzat, art. 8G, 9G (cached copy at http://webcache.googleusercontent.com/search?q=cache:PxnvWuqUMKkJ:iwiw.hu/pages/misc/privacy.jsp+&cd=2&hl=nl&ct=clnk accessed July 25, 2014); Sina FAQ. Can Weibo Be Private? http://help.sina.com.cn/comquestiondetail/view/990/.

811 Weibo has introduced a 'blacklist' function. 2 December 2009. http://blog.sina.com.cn/s/blog_61ecce970100gh66.html.

information private but then changing privacy settings and causing information to be made public inadvertently.[812]

The sheer amount of public content available on Facebook has given rise to companies like Geo Listening, which monitors 'public posts on social networks' like Facebook and Twitter to provide schools with information about their students in order to deter bullying, depression, self-harm, substance abuse and truancy.[813]

In 2014, a Berlin court ruled that several clauses of Facebook's privacy policy and terms of service violate German law.[814] The German data protection authority initiated an inquiry into facial recognition technology and raised concerns about the fact that Facebook did not notify users that facial recognition technology is being used. It also raised concerns over the potential misuse of the company's massive biometrics database. The German Data Protection Authority also held that Facebook should delete all facial recognition data already collected, and, at least, obtain consent.[815] In mid-2014, Max Schrems, a 26-year-old Austrian law student, launched a class action suit against Facebook. As of August 2014, his action had attracted 25,000 users worldwide. Schrems claims that Graph Search and data sharing by widgets on external websites violate EU privacy laws.[816]

Despite such concerns in Europe, users in countries such as Hungary are even less happy with the local alternaties; interviews with Hungarians who have used both social networks said that they generally trusted Facebook but perceived iWiW's privacy policies as deficient and 'unprofessional'.[817]

Legal implications of real-name requirements

Facebook's real-name policy has been the subject of government investigations. In Germany, Schleswig-Holstein's Data Protection Commissioner argued that Facebook had violated the Telemedia Act, which allows internet users to be anonymous or

812 Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises. Federal Trade Commission. 29 November 2011. http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

813 Geo Listening Monitoring Service Privacy Policy. last updated 10 October 2013. http://geolistening.com/privacy-policy (Accessed 8 August 2014); Stephen Ceasar. 14 September 2013. Glendale district says social media monitoring is for student safety. *Los Angeles Times*. www.latimes.com/local/la-me-glendale-social-media-20130915-story.html (Accessed 8 August 2014); Geo Listening. FAQs, under 'Can you explain privacy and social networks?' https://geolistening.com/faq

814 Facebook subject to German data protection rules, says Berlin court. *Out-law.com.* 26 February 2014. http://www.out-law.com/en/articles/2014/february/facebook-subject-to-german-data-protection-rules-says-berlin-court (Accessed 25 July 2014.); Verbraucherzentrale Bundesverband [Federation of German Consumer Organizations]. Key Statements on the Judgment by the Court of Appeal of 01/24/2014, Ref. No. 5 U 42/12. 24 January 2014. http://www.vzbv.de/cps/rde/xbcr/vzbv/key-statements-vzbv-facebook-2014-01-24.pdf

815 Jakob Jung. 16 August 2012. Facebook must destroy facial recognition data – or get users' approval, Germany decides. *ZDNet*. www.zdnet.com/facebook-must-destroy-facial-recognition-data-or-get-users-approval-germany-decides-7000002720 (Accessed 4 August 2014.)

816 Facebook privacy challenge attracts 25,000 users. *BBC News*. 6 August 2014. www.bbc.com/news/technology-28677667 (Accessed 11 August 2014.)

817 Blase Ur and Yang Wang. Online social networks in a Post-Soviet state. op cit.

pseudonymous, though a higher court reversed the decision on procedural grounds.[818] The Facebook policy led to the deactivation of activist accounts and pages during Egypt's Arab Spring protests in 2011.[819]

Weibo is now legally required to confirm the identities of its 500 million users, a challenging task it has been unable to complete, which it acknowledges as a risk in its IPO prospectus: 'our noncompliance exposes us to potentially severe penalty'.[820]

Contesting government requests for user data

There are no known cases of iWiW and Weibo contesting government demands for user data. Facebook, on the other hand, has challenged some government requests. According to data published by the company, between July-December 2013 it complied with 29 per cent of user data requests from Hungary.[821] The table below provides an overview of government requests received as well as the company's compliance rate for all countries studied in this report.

Table 6: Facebook's rate of compliance with government requests for user data in jurisdictions studied in this report

	Requests	Accounts specified	Compliance rate
Brazil	1,165	1,651	33.82%
Egypt	6	6	0%
Germany	1,687	1,950	37.88%
Hungary	38	51	28.95%
India	3,598	4,711	53.56%
Kenya	–	–	–
Russia	1	1	0%
UK	1,906	2,277	71.30%
USA	12,598	18,715	81.02%

818 Loek Essers. 23 April 2013. Facebook Can Keep its Real Name Policy, German Appellate Court Decides. *ClO Magazine*. www.cio.com/article/2386497/facebook/facebook-can-keep-its-real-name-policy--german-appellate-court-decides.html (Accessed 4 August 2014.)

819 Wessel van Rensburg. Wael Ghonim was admin of Khaled Said Facebook page. *Kameraad Mhambi.* 7 February 2011. http://mhambi.com/2011/02/ghonim-was-admin-of-khaledsaid-facebook-page (Accessed 9 July 2014); Mike Giglio ElShaheed: The Mysterious 'Anonymous' Behind Egypt's Revolt. *Newsweek.* 30 January 2011. (updated 2 February 2011)
http://www.newsweek.com/elshaheed-mysterious-anonymous-behind-egypts-revolt-66697 (Accesssed 9 July 2014); Adrian Chen. 5 February 2011.Why Facebook Should Do More to Help Egypt's Protesters. *Gawker*. http://gawker.com/5752904/why-facebook-should-do-more-to-help-egypts-protesters (Accesssed 9 July 2014.)

820 Form F-1 Registration Statement as filed with the Securities Exchange Commission by Weibo Corporation. March 14, 2014. p. 37. http://www.sec.gov/Archives/edgar/data/1595761/000119312514100237/d652805df1.htm

821 Facebook. Government requests report. Hungary. July-December 2013. https://govtrequests.facebook.com/country/Hungary/2013-H2

On user data requests, the numbers in the table above demonstrate that Facebook did not comply with all requests received.

Twitter describes itself as the 'free speech wing of the free speech party' and has cultivated a reputation for challenging government requests.[822] In 2011, it convinced a US judge to lift a gag order, allowing it to notify three WikiLeaks affiliates that their account information had been passed to US national security authorities following an official order.[823] In 2012, it failed in its efforts to challenge a law enforcement request to turn over the information of an Occupy Wall Street protester.[824] Twitter contested a subpoena in France but was ordered by a French court to turn over information on anti-Semitic accounts.[825]

Companies more often make at least some data available upon receiving government requests in the United States than in the other countries researched. This is primarily because the companies are headquartered in the United States, and wherever possible ask other governments to use the Mutual Legal Assistance Treaty (MLAT) process to channel user data requests through the US government.[826]

Official penalties against users

Users can be penalized for their online expression, and thus the potential for liability and harassment can lead to self-censorship. Social networking platforms generally remain silent when users' publicly shared information results in penalties by governments, even when the penalty is not in line with international standards for legitimate limitation of expression. Companies may be required to take action as part of the penalty such as removal of the user's content, as discussed in the previous sections.

In **China**, individuals are liable for their posts on social media. In March 2012, the government launched a 'spring breeze' campaign targeting trade in illicit goods, drugs,

---

822 Amir Efrati. Twitter CEO Costolo on Apple, Privacy, Free Speech and Google; Far From IPO. 18 October 2011.
http://blogs.wsj.com/digits/2011/10/18/twitter-ceo-costolo-on-apple-privacy-free-speech-and-google-far-from-ipo/ (Accessed 29 April 2014.)

823 Mathew Ingram. 18 October 2011. For Twitter, Free Speech Matters – Not Real Names. GigaOm. http://gigaom.com/2011/10/18/for-twitter-free-speech-is-what-matters-not-real-names (Accessed 9 April 2014); Paul Sonne. 10 January 2011. U.S. Asks Twitter for WikiLeaks Data. *Wall Street Journal*. http://online.wsj.com/news/articles/SB10001424052748704482704576072081788251562 (Accessed 29 April 2014.)

824 Russ Buettner. 2 July 2012. Judge Orders Twitter to Release Protester's Messages. *New York Times*. http://cityroom.blogs.nytimes.com/2012/07/02/judge-orders-twitter-to-release-protesters-messages (Accessed 10 August 2014); Somini Sengupta. 3 September 2012. Twitter's Free Speech Defender. *New York Times*. www.nytimes.com/2012/09/03/technology/twitter-chief-lawyer-alexander-macgillivray-defender-free-speech.html (Accessed 4 August 2014); Shira Ovide. 4 August 2013. For Twitter, Free Speech Is a High-Wire Act. *Wall Street Journal*. http://online.wsj.com/news/articles/SB10001424127887323997004578643883120559180 (Accessed 8 April 2013).

825 Angelique Chrisafis. 12 July 2013. Twitter gives data to French authorities after spate of antisemitic tweets. *The Guardian*. http://www.theguardian.com/technology/2013/jul/12/twitter-data-french-antisemitic-tweets (Accessed 9 August 2014); Somini Sengupta. 13 July 2013. Twitter Yields to Pressure in Hate Case in France. *New York Times*. www.nytimes.com/2013/07/13/technology/twitter-yields-to-pressure-in-hate-case-in-france.html (Accessed 9 August 2014.)

826 For more about the MLAT process see Google's MLAT page at https://www.google.com/transparencyreport/userdatarequests/legalprocess/ and also a resource page published by Access at https://www.accessnow.org/blog/2014/01/09/mlat-a-four-letter-word-in-need-of-reform

human and organs, as well as privacy breaches. As a result, 1,065 suspects were arrested and 200,000 messages were deleted.[827]

In India, numerous arrests have taken place under section 66A of the IT Act 2000, which criminalizes a range of online content including offensive content.[828] Yet a number of these arrests have been criticized in the media as being a violation of rights in relation to speech that was not illegal in many commentators' view. For example, in 2012, two Air India employees were arrested in Mumbai and jailed for 12 days after posting derogatory comments on Facebook about city-wide commemorations of the death of the leader of a religious political party.[829]

In the **United States**, a user of both Facebook and Twitter was arrested and charged for posting information on the social networks that were perceived as terrorist threats.[830] He was an 18-year-old high school student and aspiring rapper who posted controversial lyrics on Facebook that could – in the opinion of some, depending on the context – be construed as announcing a plan for an attack on a city. He was released by a grand jury.[831]

5.5 Transparency

This section examines the policies and practices of companies related to transparency, building on information about transparency reports and other practices already discussed in previous sections.

5.5.1 Transparency about government and lawful requests

As mentioned earlier in this study, both Facebook and Twitter publish data sets that have come to be known as 'transparency reports'. Section 5.3.1 included a comparative analysis of data published by Facebook and Twitter about government requests to restrict user content.

Facebook's 'Government Request Report' first disclosed information about content restriction in April 2014 (its previous report only disclosed user data requests).[832]

827 "Beijing arrests 1,000 in Internet crime crackdown", *ChinaDaily*, 31 March 2012, http://www.chinadaily.com.cn/china/2012-03/31/content_14962187.htm.
828 Information Technology Act 2000 as amended in 2008. Section 66A.
829 Shipla Jamkhandikar. 19 November 2012. No criticism please, we are Indians. *Reuters: India Insight*. http://blogs.reuters.com/india/2012/11/19/no-criticism-please-we-are-indians and Saurabh Gupta. 2 December 2012. Facebook row: Mumbai Police book man whose complaint led to Air India employees' arrests. *NDTV*. www.ndtv.com/article/india/facebook-row-mumbai-police-book-man-whose-complaint-led-to-air-india-employees-arrests-299898 (Accessed 4 August 2014.)
830 Craig Malisow. 12 February 2014. A Young Man's Violent Threat on Facebook Lands Him in Jail, and Limbo. *Houston Press*. www.houstonpress.com/2014-02-13/news/justin-carter-facebook/full/ (Accessed 11 April 2014.)
831 Eric Randall. The Methuen Teen Rapper Was Released from Jail. *Boston*. 7 June 2013. www.bostonmagazine.com/news/blog/2013/06/07/the-methuen-teen-rapper-was-released-from-jail (Accessed 11 April 2014.)
832 Facebook Government Requests Report. About the Reports. https://govtrequests.facebook.com/about.

As described in section 5.3.1, Facebook only reports the number of government requests that it complied with but does not report on the total number of government requests received. It also does not include court orders or copyright takedown notices in its figures. As reflected in section 5.4.2, Facebook's transparency report provides much more detail about government requests for user data – including information about compliance rate and request types – than its very basic and incomplete information about content restriction requests.

Twitter has disclosed content removal requests since its first transparency report in 2012. In addition to what Facebook discloses, Twitter's report also includes compliance rate, content withheld as well as copyright takedown notices.[833] Twitter also distinguishes itself from Facebook in transparency about content restriction by publishing copies of the content restriction and takedown requests it receives to the Chilling Effects website (see Study 2 for a discussion of Chilling Effects).[834] For its reporting on government data requests Twitter also provides details on types of requests and compliance rate, as well as data about information disclosed to authorities during emergencies.[835]

The two US-based companies face constraints on what their home government will permit them to report. The US government does not permit US companies to be completely transparent about National Security Letters and FISA court orders.[836] With the NSA revelations, transparency mechanisms have become a point of debate. The issue is to understand the scope of how users' privacy is affected at a time when companies have publicly expressed concern about how erosion of user trust in the internet diminishes its commercial value.[837] A number of US companies including Facebook have negotiated an agreement with the US Government that allows them to report requests with a one-year delay and in broad ranges, not exact numbers of requests received. Twitter was also a part of that coalition but has signalled its dissatisfaction with the arrangement, arguing that 'these ranges do not provide meaningful or sufficient transparency'.[838]

---

833 For more information about the Digital Millennium Copyright Act see legal summaries in Chapter 2.

834 'Chilling Effects' is a website that allows recipients of 'cease and desist' notices to submit the notice to the site and receive information about their legal rights. For more information about Twitter's practice of sharing information with 'Chilling Effects' see: https://transparency.twitter.com/removal-requests/2013/jul-dec. For more information about 'Chilling Effects' see: http://www.chillingeffects.org. Information about instances of Twitter being blocked is from Herdict.com and includes information from China and Iran – two countries where Twitter is was blocked at the time of writing. Twitter Transparency Report. Additional information. https://transparency.twitter.com/additional-information

835 Twitter clarifies that the company evaluates 'emergency disclosure requests' on a case by case basis as per US law and if the company has good faith to believe that there is an emergency involving the danger or death or serious physical injury to a person. For more information see: https://support.twitter.com/articles/41949#12.

836 Karen Gullo. 7 October 2014. Twitter Sues U.S. Over Transparency on National Security. Bloomberg. http://www.bloomberg.com/news/2014-10-07/twitter-sues-u-s-over-transparency-on-national-security.html (Accessed 25 July 2014.)

837 Seth Rosenblatt. 8 October 2014. US spying scandal will 'break the Internet,' says Google's Schmidt. CNet.
http://www.cnet.com/news/us-spying-scandal-will-break-the-internet-says-googles-schmidt/ (Accessed 9 October 2014.)

838 Jeremy Kessel. 6 February 2014. Fighting for more #transparency. Twitter Blog. https://blog.twitter.com/2014/fighting-for-more-transparency (Accessed 8 August 2014.)

Weibo does not publish a transparency report because government requests fall under China's State Secrets Law. Due to legal constraints, it appears that the offline and online media rarely mention state-level restrictions of content.[839]

iWiW did not publish any type of transparency report before its operations closed down.

5.5.2 Transparency about self-regulation

While Facebook and Twitter have taken efforts at increasing transparency about how they handle government and lawful requests, they share much less information with users or the public at large about how they enforce their own terms of service. None of the companies studied provide information on content they have restricted based on company policy, or any statistics about external reporting on violations of company rules. As previously noted in earlier sections, government authorities in many countries may avail themselves of mechanisms for reporting terms of service violations, but no data about the number, source, or subject matter has been reported by either of these companies. In fact, Facebook explicitly states in that it excludes from its government requests report, 'government requests to remove content that violates Facebook's Community Standards, such as child exploitation material'.[840]

While all social networks list content they prohibit, none of the companies studied has provided much public information about procedures for evaluating content. Industry sources have described internal rules and procedures for evaluating content in conversations with concerned stakeholders, held on condition of non-attribution, but such processes are generally not made public.[841] It is usually through anecdotal evidence via news reports that the public learns about specific examples.

5.5.3 User notification

Companies are inconsistent in informing users when they restrict their content or hand over their user data. If content is removed due to a copyright violation, both Twitter and Facebook are legally required under the DMCA to notify the user and provide information on how to file a counter-notice.[842] Furthermore, both companies commit to inform users

---

839 Mitchell A. Silk and Jillian S. Ashley. 1 January 2011. Understanding China's State Secrets Laws. *China Business Review*. www.chinabusinessreview.com/understanding-chinas-state-secrets-laws (Accessed 10 August 2014); Beina Xu. 12 February 2014. Media Censorship in China. *Council on Foreign Relations*. www.cfr.org/china/media-censorship-china/p11515. (Accessed 4 August 2014); Shi Shan. 10 July 2014. China's Media Ban on Reporting of State Secrets 'Too Vague'. *Radio Free Asia*. www.rfa.org/english/news/china/vague-07102014155503.html (Accessed 10 August 2014.)

840 Facebook. Government requests report. FAQ. https://govtrequests.facebook.com/faq

841 oDesk. Abuse Standards 6.2 - Operation Manual. http://www.scribd.com/gawker/d/81877124-Abuse-Standards-6-2-Operation-Manual (Accessed 30 July 2014.)

842 Twitter. Transparency Report. Copyright notices. July-December 2013. https://transparency.twitter.com/copyright-notices/2013/jul-dec; Facebook. Desktop Help. What happens when Facebook acts on a claim that I have infringed someone's copyright? Can I file a counter-notice? https://www.facebook.com/help/365111110185763.

about about requests for their data, unless the situation is an emergency or the company is legally prohibited to do so.[843]

For content that Facebook removes to enforce its own Community Standards and Statement of Rights and Responsibilities (SRR), the company commits to forewarn people,[844] but Twitter does not clarify if it does the same for content that violates its terms.[845] If it implements a foreign content restriction request, Twitter notifies the public about the restriction through a 'Tweet withheld' notice, which it also uses for copyright-related takedowns:[846]

As mentioned previously, Twitter only restricts accounts in the jurisdiction whose authorities made a valid request. In such cases it displays the following notification:

Facebook displays a more generic message such as the following from July 2014:

The text in the above message could mean many things and it is unknown which one applies to a particular situation.

When content is restricted on Weibo, other users trying to access the post are notified: 'I'm sorry, this post has been deleted. For more information, go to [link provided].'

---

843 Twitter. Help Center. Guidelines for Law Enforcement. https://support.twitter.com/entries/41949; Facebook. Safety Center. Information for Law Enforcement Authorities. https://www.facebook.com/safety/groups/law/guidelines.

844 Facebook. Desktop Help. About Facebook's Security & Warning Systems. https://www.facebook.com/help/365194763546571/.

845 Twitter. Help Center. Twitter media policy.https://support.twitter.com/articles/20169199-twitter-media-policy; Help Center. The Twitter Rules https://support.twitter.com/articles/18311-the-twitter-rules ; terms of service. 25 June 2012. https://twitter.com/tos.

846 Twitter. Help Center. Country Witheld Content. https://support.twitter.com/articles/20169222-country-withheld-content

Weibo has been reported by users to 'camouflage' messages so they remain visible only to the author, causing some authors to be unaware that their content was restricted.[847] When Weibo deleted dissident artist Ai Weiwei's account, it was replaced with a message that read: 'Error. Invalid Weibo user'.[848]

5.6 Remedy

None of the companies investigated offer a clear path to remedy for users who face image or text removal or functional restrictions, such as the user's inability to upload photos.

Facebook may remove pages (which tend to belong to businesses and organizations that may buy advertisements) for alleged spam violations, but users have options to appeal.[849]

In one of the countries studied, the law does require some form of grievance mechanism: India's Intermediary Guidelines require intermediaries to have 'grievance officers' to whom users may address privacy concerns and harassment claims.[850]

Facebook recommends using the help center's web forms, but Indian users can contact a grievance officer via email or postal mail (this information is not displayed to users outside of India).[851] Twitter has a grievance officer whose contact information is visible to users outside India.[852]

For suspended accounts, both Twitter and Facebook do offer an appeal option. When accounts are disabled for reasons of violating Facebook's Statement of Rights and Responsibilities, users can send an appeal through a specific form. There is no information about how long it will take for a request to be processed, what the decision-making procedure is, or the severity of violations that would trigger an account suspension.[853] Twitter's information page is also short on such information but explains more about how to appeal.[854] One exception is copyright, as US copyright law (the DMCA) requires Twitter

---

847 Oiwan Lam. 18 March 2013. China: Researchers Uncover Microblog Filtering Mechanisms. http://advocacy.globalvoicesonline.org/2013/03/18/china-researchers-uncover-microblog-filtering-mechanisms (Accessed 25 July 2014); Some behaviors of deleting Weibo message secretly have been found and made public by users. http://weibo.com/1221117947/zdHlw7sCK?mod=weibotime.

848 Sui-lee Wee. 19 March 2012. Ai Weiwei says censors removed his microblog. *Reuters*. www.reuters.com/article/2012/03/19/us-china-artist-microblog-idUSBRE82I09U20120319 (Accessed 10 August 2014.)

849 Facebook. Desktop Help: Managing a Page. Why are there limits on my Facebook Page? https://www.facebook.com/help/348805468517220

850 Information Technology (Intermediaries guidelines) Rules, 2011, 11 April 2011. http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf, §11; Display grievance officer's name, contact: HC to Google, FB. *Hindustan Times*. 23 August 2013. www.hindustantimes.com/india-news/newdelhi/display-grievance-officer-s-name-contact-hc-to-google-fb/article1-1111939.aspx (Accessed 27 July 2014.)

851 Facebook. Desktop Help. Contact Your Grievance Officer. https://www.facebook.com/help/253918971400132 .

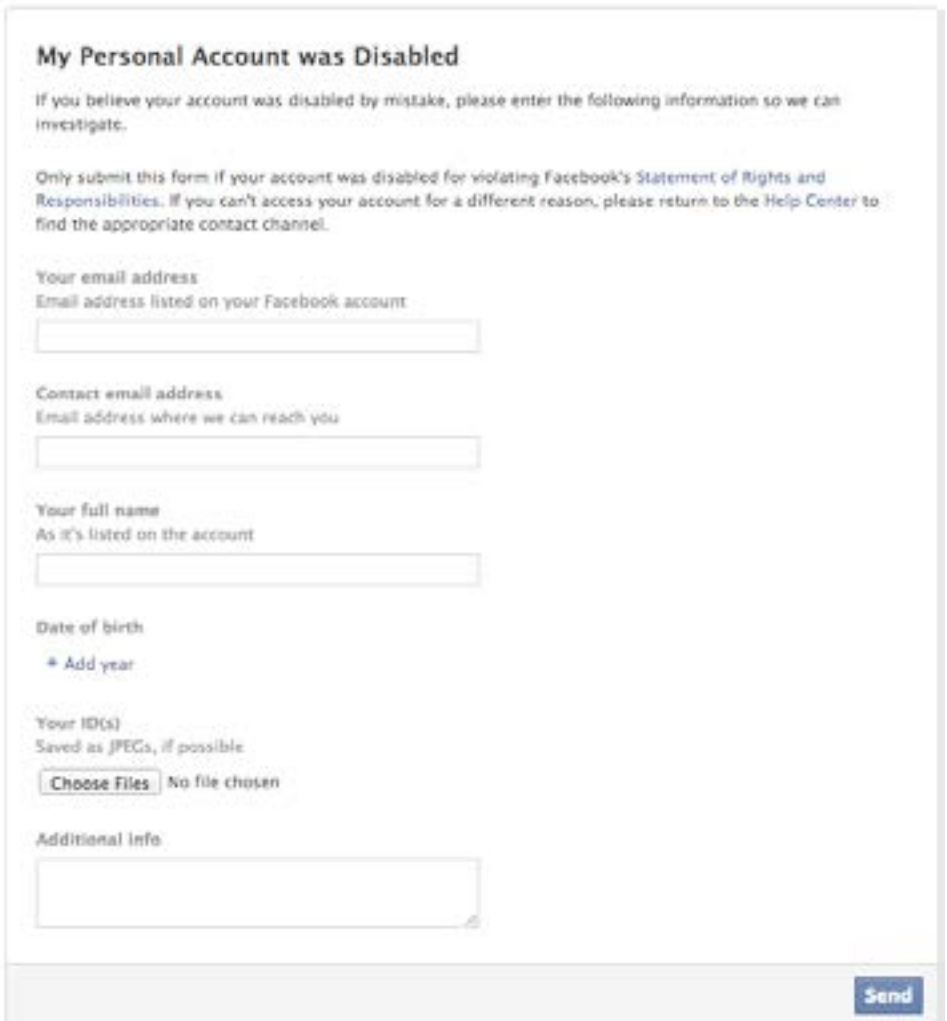
852 Twitter. Help Center. Grievance Officer – India. https://support.twitter.com/groups/57-safety-security/topics/275-handle-issues-online/articles/20171602-grievance-officer-india.

853 Facebook Desktop Help. My Personal Account was Disabled. https://www.facebook.com/help/contact/260749603972907.

854 Twitter. Help Center. My account is suspended. https://support.twitter.com/articles/15790-my-account-is-suspended.

and Facebook to notify the original content uploader and inform them about counter-notices.[855] It is unclear what sort of paths to remedy iWiW offered, if any.

Figure 11: Screen shot of form that users can use to appeal Facebook account suspensions.[856]



855 Facebook. Desktop Help. What happens when Facebook acts on a claim that I have infringed someone's copyright? Can I file a counter-notice? https://www.facebook.com/help/365111110185763; Twitter. Help Center. Copyright and DMCA policy. https://support.twitter.com/articles/15795-copyright-and-dmca-policy.

856 Screen shot 27 July 2014. Facebook. Desktop Help. My Personal Account was Disabled. https://www.facebook.com/help/contact/260749603972907.

Weibo does not offer a direct appeal option or a web form; instead, users are encouraged to email the company and to indicate if they 1) disagree about administrators' operations; 2) are dissatisfied with administrators' responses after communication; 3) have questions relating to other administrative matters.[857]

On Weibo sparse information about remedies has meant largely having to rely on anecdotal evidence. Content restriction seems to be inconsistent. For example, blogger and free speech advocate Isaac Mao had his account closed in June 2012 after he criticized China's space program. Sina was reported to have told him he had no recourse to appeal because the order had been given by 'relevant authorities', and was outside the company's control.[858] Author Zhang Yaojie's Weibo account was closed in September 2012. Following months of unsuccessfully navigating the online complaint system, Zhang sued Sina in January 2013 for a refund of his monthly 10 yuan ($1.61) premium membership fee and account reinstatement.[859] Court delays lasted months, and at the time of writing no action seemed to have been taken.[860]

5.7 Conclusions

In analyzing the interplay between intermediaries' policy and practice and specific national regulatory and legal contexts, the research shows that companies are better able to maximize respect for internet users' rights in jurisdictions where laws are relatively compatible with international human rights norms regarding freedom of expression and privacy. The legal context of the country in which a company is headquartered is particularly important for the respect of user rights. Companies whose home governments do not inhibit such efforts have made strides in transparency and accountability in terms of how they handle government demands.

Yet the research also clearly shows that freedom of expression can be strongly influenced in a positive or negative direction by companies' own rules, processes and mechanisms on matters including terms of service enforcement, user privacy and identity. Companies are much less transparent and accountable with the public on these matters.

In general the research conducted for this study of Facebook, Twitter, Weibo and iWiW points to the following conclusions:

Government actions against social network users may limit space for expression. Facing fines or even arrests, users are sometimes penalized by some governments for their online expression. A lack of clarity on what expression is and is not allowed, and

857 Sina Help. Complaints to a Weibo Manager. http://help.sina.com.cn/comquestiondetail/view/1077

858 Sophie Beach. 11 March 2013. Challenged in China. CPJ.org. http://cpj.org/reports/2013/03/challenged-china-media-censorship-weibo-expression.php (Accessed 12 Sepbember 2014.)

859 Josh Ong. 24 January 2013. Chinese scholar sues Sina over Weibo microblog account closure. http://thenextweb.com/asia/2013/01/24/chinese-scholar-sues-sina-over-weibo-microblog-account-closure/

860 Zhang Yaojie. 1 May 2013. Please carry out the right to 'hashly criticize'. My1510. http://www.my1510.cn/article.php?id=96400; Phone interview with Mr. Zhang and e-mail interview with his lawyer, Wang Zhenyu, 15 April 2014.

restrictive policies can lead to self-censorship by users. Companies that operate social networking platforms can help by being clear and transparent with users about their content restriction practices, privacy settings, and data sharing policies. Companies can also support individuals targeted in cases where penalties are not in line with international human rights standards.

In some circumstances, companies can contest or decline removal requests. Establishing guidelines and 'best practice' standards helps. As is evident in Twitter's transparency report, social networks do not necessarily comply with all requests for content removals; in fact Twitter has only complied with 11 per cent of such requests. This shows that social networks do have operating space to challenge content restriction requests. It may be easier to resist pressures from countries other than the network's home jurisdiction, but even within the home country, some companies do not comply with all requests. Of the four social networks profiled here, only two (Twitter, Facebook) publish their criteria, if not the actual process, for dealing with content removal requests from governments and/or third parties. Such published policies help users understand in what circumstances their content may be removed by external request, and can give companies a clearer framework to contest content removal demands that are not consistent with due process or international human rights

Social networks are inconsistently transparent on government removal requests. Only two of the four social networking platforms studied (Twitter and Facebook) provide information about government requests, shedding an important light on how law is enforced on their platforms. Twitter also shares the content removal request itself, where possible, with the 'Chilling Effects' website and notifies the public via messages on the platform when content is restricted based on request by a government. Across jurisdictions studied in this research, governments are not fully transparent about the nature and scope of content restriction and requests for user data on social media platforms.

Some social networks do not always explain how they share user data with authorities and others. Two of the four companies studied (Facebook, Twitter) have published policy guidelines on how they respond to user data requests from both foreign and domestic authorized bodies. Users of the other services are not informed how their privacy will be protected in the face of requests by governments or others.

None of the companies in this case study publish data on self-regulatory restrictions – e.g. how many accounts were disabled for impersonation, how many accounts of repeat infringers were terminated, etc. With social networking platforms increasingly becoming a central platform to individuals' online expression, there is a strong interest among users and stakeholders in having rules and enforcement processes that are clear, predictable and to some degree, independently monitored. The absence of such accountability detracts from intermediaries' credibility and legitimacy as platforms for users' freedom of expression.

Users' vulnerability places special responsibility on social networks to protect users' privacy. With the significant amount of personal information available through social network use, social networks carry a special responsibility to respect users' right to privacy. Lack of privacy protection may stifle individuals' expression.

"Real name" policies require flexible implementation in order to avoid negative impacts on users' freedom of expression. Real-name requirements may have a serious chilling effect on speech. China legally requires social networks to verify their users' identities, but this is not the case in most jurisdictions. The authors recommend that companies consider the privacy and free expression ramifications of implementing a real-name policy (or enter the market of a country with such laws) by conducting a human rights impact assessment.

There is a need for stronger global principles and guidelines for remedy and transparency in self-regulation. The Global Network Initiative's principles on freedom of expression and privacy and accompanying implementation guidelines have provided strong guidance, supported by a range of stakeholders, not only for GNI companies but for internet intermediaries more broadly. GNI's guidelines for companies on transparency and process for handling government requests, grounded in international human rights norms, have had an impact on company practices all three intermediary types studied in this report. However this study highlights the glaring absence of similar principles, guidelines and standards for companies' self-regulatory practices, including terms of service enforcement. Given the lack of transparency and consistency in how companies enforce their terms of service and other private rules, and given the impact of such enforcement of internet users' freedom of expression, there is a clear need for the development of guidelines and 'best practice' standards for intermediaries' own rules on user expression.

6. GENDER

Among the 81 countries covered by the World Wide Web Foundation's 2013 Web Index, only half of had national policies addressing gender equality online. The authors of the 2013 Web Index report point out that a "Lack of political and policy focus is compounded by failure to collect gender-disaggregated statistics." As a result, 'the ways in which gender affects Web access and use are still poorly understood'.[861] This chapter begins with a brief overview of the issue of basic internet access for women in relation to men, followed by an examination of how content restriction in some countries has affected womens' access to health information and gender-related discourse. The final section discusses issues related to pernicious harassment targeting women and how it that affects womens' freedom of expression online by chilling their participation in the digital information society more broadly.

6.1 Access to the internet

The extent to which internet empowers women cannot be underestimated and has been highlighted by several reports that point to opportunities for empowerment, including, gender equality, and economic benefits to women. Yet globally there is a significant gender divide in broadband access between men and women. Factors affecting women's access to broadband include educational and income gaps, and that these factors are more acute for women in developing countries versus women in developed countries.[862] For example, in 2013 Google India found that though India houses over 200 million internet users, only 60 million of these online users are women.[863]

Similarly, penetration of internet was 32 per cent for women in Egypt with 41 per cent of the Egyptian women not being interested in the internet and another 23 per cent feeling that they do not need access to the internet. Of this group, 22 per cent do not use the internet due to fear that friends or family would disapprove or that it is not appropriate to use the internet.[864] In Brazil, 47 per cent of active internet users are women. In Kenya,

---

861 Anne Jellema and Karin Alexander. 22 November 2013. *2013 Web Index Report*. Geneva, World Wide Web Foundation, p. 20. http://thewebindex.org/wp-content/uploads/2013/11/Web-Index-Annual-Report-2013-FINAL.pdf

862 Broadband Commission Working Group on Broadband and Gender. September 2013. *Doubling Digital Opportunities: Enhancing the Inclusion of Women & Girls in the Information Society*. Geneva, International Telecommunications Union. www.broadbandcommission.org/Documents/working-groups/bb-doubling-digital-2013.pdf ; Intel Corporation and Dalberg Global Development Advisors. 2012. *Women and the Web: Bridging the Internet Gap* and *Creating New Global Opportunities in Low and Middle-Income Countries*. www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf

863 *The Economic Times*. 20 November 2013. Google India aims to bring 50 million women online. http://articles.economictimes.indiatimes.com/2013-11-20/news/44284934_1_google-india-internet-new-campaign-aims (Accessed 28 July 2014.)

864 Intel's 'Women and the Web' report highlights online habits in Egypt, Uganda. 13 January 2014. oAfrica. www.oafrica.com/statistics/intels-women-and-the-web-report-highlights-online-habits-in-egypt-uganda (Accessed 31 July 2014.)

fewer than 28 per cent of citizens had internet access in 2013. The lack of access and adequate internet infrastructure affects low-income rural areas the most, and women most severely. Further, a study conducted in 2013 demonstrated that only 8 per cent of respondents used the internet to access news.[865] In contrast, in 2013 in the UK 84 per cent of women over 16 years old had access to the internet.[866] Also seen is a growing trend of women increasingly accessing internet through smart phones. In Germany a study found that the use of smartphones by German women increased by over 60 per cent in 2013, while use by men increased only by 35 per cent.[867] Policy interventions that states can take to overcome the gender gap include expanding access to affordable platforms, developing national plans to allow for increased broadband penetration, and addressing market constraints that impact the affordability of internet platforms.[868]

6.2 Gender and content restriction

In some countries, women's rights advocates are demanding broader restrictions on pornographic and 'obscene' content online, arguing that there is a connection between the online viewing of such materials and violence against women.[869] In connection with this, the ISP case study (Chapter 3) describes debates in India and the UK on whether and how to institute ISP filtering.

In some countries, laws meant to curb pornography are also used to stamp out other content. The Chinese Government, for example, periodically announces months-long campaigns to rid the Chinese internet of pornography and 'vulgarities' that are 'violating

865 Victoria Rocío Cunto, Moses Osani and Hannah Smothers. 2013. *Empowerment Through Internet Access: Promoting Women's Rights with Social Media*. Salzburg Academy on Media and Global Change. www.salzburg.umd.edu/unesco/empowerment-through-internet-access (Accessed 28 July 2014.)

866 UK Government. 19 February 2014. Internet Access Quarterly Update, 2013 Q4. Office for National Statistics. www.ons.gov.uk/ons/publications/re-reference-tables.html?edition=tcm%3A77-300202#tab-all-tables

867 comScore. 14 March 2013. 2013 Future in Focus – Digitales Deutschland. www.comscore.com/ger/Insights/Presentations_and_Whitepapers/2013/2013_Future_in_Focus_Digitales_Deutschland (Accessed 30 May 2014.)

868 Broadband Commission Working Group on Broadband and Gender. September 2013. *Doubling Digital Opportunities: Enhancing the Inclusion of Women & Girls in the Information Society*. Geneva, International Telecommunications Union. www.broadbandcommission.org/Documents/working-groups/bb-doubling-digital-2013.pdf; Intel Corporation and Dalberg Global Development Advisors. 2012. *Women and the Web: Bridging the Internet Gap* and *Creating New Global Opportunities in Low and Middle-Income Countries*. www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf

869 Mary Eberstadt and Mary Anne Layden. 2010. *The Social Costs of Pornography: A Statement of Findings and Recommendations*. Princeton, N.J., The Witherspoon Institute; Catharine A. MacKinnon and Andrea Dworkin. 1988. *Pornography and Civil Rights: A New Day for Women's Equality*. Minneapolis, Organizing Against Pornography; Milton Diamond. 1999. The Effects of Pornography: an international perspective. James Elias, Veronica Diehl Elias, Vern L. Bullough, Gwen Brewer, Jeffrey J. Douglas and Will Jarvis (eds). *Porn 101: Eroticism, Pornography, and the First Amendment*. Amherst, N.Y., Prometheus Books.

public morality and harming the physical and mental health of youth'.[870] During one of these campaigns in 2009, the Beijing Communications Administration shut down 'Bullog', a popular blogging community due to 'harmful comments on current affairs'.[871] Baidu and Google were also on a list of target websites required to clean up their content.[872] Another campaign launched in April 2014 targeted amateur online romance stories, many of which were 'slash fiction', or male same-sex romances written for female audiences (a similar crusade in 2012 landed approximately 20 women in jail for up to 18 months.)[873] Although some officials praised this as the coming of 'rule of law in the virtual world',[874] some experts have argued for an amendment to the definition of 'online pornography' in order to avoid restricting freedom of expression.[875]

Our research team found that content related to women's rights and medical information is generally not restricted by Internet companies including search engines. However companies continue to struggle for the right balance in relation to broad laws that can be subject to a wide range of possible interpretation. For example, in November 2013 the Gender Studies Group of Beijing Foreign Studies University (BFSU) posted 17 photos on social network Renren.com. On each photo, there was a female student holding a whiteboard and expressing her idea about sex with title starting with "My vagina says". Organizers and participants said their activity was inspired by Eve Ensler's feminist play, *The Vagina Monologues*.[876] The BFSU students provoked hot debate on the Chinese

---

870 Chris Buckley. 5 January 2009. China targets big websites in Internet crackdown. Reuters. www.reuters.com/article/2009/01/05/us-china-internet-idUSTRE5040F120090105 (Accessed 31 July 2014); China Internet Illegal Information Report Centre. 5 January 2009. State Council Information Office and Other Six Ministries Carry Out Special Campaign against Internet Vulgarities. http://net.china.com.cn/ywdt/txt/2009-01/05/content_2668979.htm (Accessed 28 July 2014); Michael Wines. 12 March 2009. A Dirty Pun Tweaks China's Online Censors. *New York Times*. www.nytimes.com/2009/03/12/world/asia/12beast.html (Accessed 28 July 2014.)

871 Tania Branigan and Jemima Kiss. 13 January 2009. China closes 90 websites as internet crackdown intensifies. *The Guardian*. www.theguardian.com/media/2009/jan/13/china-internet-censorship (Accessed 28 July 2014); Anita Chang. 9 January 2009. Edgy China blog site shut amid Internet porn sweep. Fox News. www.foxnews.com/printer_friendly_wires/2009Jan09/0,4675,ASChinaPornography,00.html (Accessed 31 July 2014); Wang Xiao. 28 February 2007. The Story Behind One of China's Largest Blogging Communities. *The Blog Herald*. www.blogherald.com/2007/02/28/the-story-behind-one-of-chinas-largest-blogging-communities (1 August 2014.)

872 People's Daily Online: *The First List Of Websites Under Exposure During the National Campaign against Internet Vulgarities*, January 5, 2009, http://politics.people.com.cn/GB/1026/8622333.html.

873 Alia. 16 April 2014. Slash fiction falls victim to China's latest crackdown on online porn. Offbeat China Blog. http://offbeatchina.com/slash-fiction-falls-victim-to-chinas-latest-crackdown-on-online-porn (Accessed 1 August 2014); Liu. 17 May 2012. '扫黄打非'办：耽美小说网负责人获刑1年半. ['Pornography': slash fiction network executives jailed for a year and a half]. *China Youth Daily*. (In Chinese.) http://news.china.com/focus/zhengzhidisu/11115954/20120517/17201391.html (Accessed 1 August 2014); Kevin Tang. 22 April 2014. Inside China's Insane Witch Hunt For Slash Fiction Writers. *BuzzFeed*. www.buzzfeed.com/kevintang/inside-chinas-insane-witch-hunt-for-slash-fiction-writers (Accessed 1 August 2014.)

874 Xinhua. 16 April 2014. Porn crackdown crucial to cyber development: experts. *Global Times*. www.globaltimes.cn/content/854927.shtml (Accessed 31 July 2014.)

875 Abby Liu. 3 May 2014. China's Anti-Pornography Crackdown Nets Much More Than Porn. *Global Voices*. http://globalvoicesonline.org/2014/05/03/chinas-anti-pornography-crackdown-nets-much-more-than-porn (Accessed 28 July 2014.)

876 NetEase: *Beijing Foreign Studies University Girls Posted Bold Photos to Express Bravely Their Opinions about Sex, "The Vagina's Way" Became a Hit*, November 7, 2013, http://henan.163.com/13/1107/23/9D4606BU022701R8.html.

Internet not only about female sexuality but also about whether it should or should not be publicly expressed by young women.

In this context it is interesting to note that a search for the word "vagina" on Baidu yields a first page full of medical and encyclopedia web pages. However as of August 2014 on Google.com.hk, the word "vagina" was blocked by the site's SafeSearch feature.[877] Users from the rest of China outside Hong Kong are not allowed to shut down this feature.

Thus in this particular case, Baidu was found to be less restrictive than Google.

Social networks' treatment of female nudity has also been a huge point of contention. Facebook's ban on breastfeeding drew user outcry.[878] After a campaign by womens' advocacy groups called #FreeTheNipple, Facebook clarified its nudity policy and decided to allow breastfeeding photos on Facebook.[879]

The examples above illustrate how women's ability to access and disseminate information and ideas about sexuality can be stifled by restrictions, and how legislation whose purpose includes protection of women can be appropriated for other purposes. However as the following section will show, some women can also feel that their rights have been violated when intermediaries fail to restrict content that has been posted on the Internet with the express intention of harming them.

6.3 Gender-based harassment

Forms of harassment that can take place via social media platforms include stalking, hate speech via graphics or text, cyber mobbing,[880] revenge porn,[881] unwanted sexual attention and sexual coercion. Indeed, harassment has become so pervasive for 'adults who are active members of at least one social network' that Zurich Insurance Group is offering a yearly 'Cybermobbing Insurance' plan for CHF 149 (approximately $165) for those who seek protection from being 'defamed, harassed or even coerced by other people via electronic channels'.[882]

---

877 Experiment conducted by the report's China researcher, June 30, 2014.

878 Mariya Yefremova. 14 April 2013. In Support of an 'Explicit Material' Prompt on Facebook. *Huffington Post*. www.huffingtonpost.com/mariya-yefremova/in-support-of-an-explicit_b_3076354.html (Accessed 10 August 2014.)

879 Kashmira Gander. 12 June 2014. #FreeTheNipple: Facebook allows breast feeding photos in change to nudity and pornography policy. *The Independent*. www.independent.co.uk/life-style/health-and-families/health-news/freethenipple-facebook-allows-breast-feeding-photos-in-change-to-nudity-and-pornography-policy-9532695.html (Accessed 4 August 2014); Facebook. Desktop Help. Does Facebook allow photos of mothers breastfeeding? https://www.facebook.com/help/340974655932193.

880 Cyber mobbing includes defamation, harassment and coercion that takes place over the internet, in chat rooms, instant messaging and mobile communications.

881 Revenge porn is sexually explicit material that is shared online without the consent of the individual.

882 Cybermobbing Insurance. Zurich Insurance Group. www.zurich.ch/en/private-customers/liability-and-legal/cybermobbing-versicherung#im-detail (Accessed 30 July 2014.)

6.3.1 Regulation

Because of the ease with which harassment and threats can take place via social media platforms, debates have arisen around the responsibility of intermediares to help prevent and address harassment. New regulations are also being drafted in many countries to address the problem. Researchers for this report found that some countries do not have legislation explicitly addressing online sexual harassment. Others have broad provisions that could potentially encompass online sexual harassment, while others have developed more specific laws.[883]

In the **United States**, the Violence Against Women Act penalizes someone who 'utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with the intent to annoy, abuse, threaten or harass any person at the called number or who receives communications' with fines or imprisonment.[884] **Germany** is considering expanding penal sanctions against online harrassment with a particular focus on incidents that take place on social networks, and also to make it easier for victims to report incidents to the police.[885] In **Brazil**, as a result of online harassment, the Marco Civil da Internet includes Article 21 which holds content providers liable if they do not remove, after being notified, videos and photos containing nudity and sex posted without the individual's consent. In this case there is no need for judicial notification. It is an exception to the 'judicial notice-and-takedown' framework established by the Marco Civil (as discussed in more detail in the intermediary liability section in Chapter 2).[886] In June 2014, the Egyptian Government criminalized sexual or

---

883 Examples: For Kenya see s. 29 of the Kenya Information and Communication Act. For India, a number of sections of the Indian Penal Code can be used to address online sexual harassment, including: IPC section 509: Addresses 'insulting the modesty and intruding on the privacy' of women, IPC Section 507: Criminal intimidation via anonymous communication, IPC Section 354A: Addresses online and offline sexual harassment, IPC Section 354C: Addresses voyeurism, IPC Section 354D: Addresses stalking including cyber stalking, Information Technology Act section 66A: can be used to address cyber-stalking and sexual harassment.

884 47 U.S.C.A. § 223(a)(1)(C). At its passage, the statute stirred significant controversy given its inclusion of the term 'annoy' because the term might capture a wide range of anonymous internet banter that falls short of cyber-stalking. Naomi Harlin Goodno. 2007. Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws. *Missouri Law Review, Vol. 72, No. 1, pp. 125–197.* http://scholarship.law.missouri.edu/cgi/viewcontent.cgi?article=3985&context=mlr; Daniel J. Solove. 9 January 2006. Response to Kaimipono D. Wenger. 9 January 2006. Annoy someone online (anonymously); go to jail. *Concurring Opinions.* www.concurringopinions.com/archives/2006/01/annoy_someone_o.html/comment-page-1#comment-61010 (29 July 2014.) Courts have responded to this controversy, finding that although the statute might have unconstitutional applications, it would not warrant facial invalidation on vagueness or overbreadth grounds. *United States v. Eckhardt, 466 F.3d 938, 943–44 (11th Cir. 2006).* http://caselaw.findlaw.com/us-11th-circuit/1467437.html (Accessed 28 July 2014.)

885 Bundesregierung. 13 December 2013. *Deutschlands Zukunft gestalten: Koalitionsvertrag zwischen CDU, CSU und SPD* [Making Germany's Future: Coalition Agreement between the CDU, CSU and SPD]. Berlin, Press and Information Office of the Federal Government, p. 147. (In German.) www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf;jsessionid=3B84643BFC5B2B3D59DBDD25CFA31216.s4t1?__blob=publicationFile&v=2

886 Ronaldo Lemos, Director, Center for Technology and Society, Fundação Getúlio Vargas (FGV) School of Law. Interview with Celina Beatriz Mendes de Almeida. Personal interview. Rio de Janeiro, Brazil, 10 April 2014.

pornographic suggestions or hints through words, signs, or acts as part of new legislation addressing the problem of sexual harassment in society more broadly.887

A specific category of online harassment increasingly discussed by policymakers and gender rights advocates is called 'revenge porn'. Perpetrators are often bitter ex-spouses or partners, or online 'trolls' who upload 'nude or sexually explicit photographs or videos of people online without their consent, even if the photograph itself was taken with consent'.[888] In an interview Brazilian Congressman Alessandro Molon, who served as the rapporteur of the Marco Civil,[889] observed that 'revenge porn' has become 'increasingly frequent' in Brazil – hence the public support for special provisions in the Marco Civil.[890]

Israel was the first country to ban revenge porn, in January 2014.[891] As of June 2014, Japan[892] and Canada[893] were also working on measures to address revenge porn. The US-based Cyber Civil Rights Initiative's 'End Revenge Porn' campaign seeks to criminalize revenge porn – at the time of writing, US victims were only entitled to civil remedies.[894] But in May 2014, Arizona became the first state to classify revenge porn as a felony.[895]

Revenge porn also afflicts emerging economies. In China, victims have turned to the courts, invoking the Article 36 of China's Tort Liability Law.[896] Two different articles of China's Criminal Law have been applied in these cases and in 2009 a man who posted

---

887 Patrick Kingsley. 6 June 2014. Egypt criminalises sexual harassment for first time. *The Guardian*. www.theguardian.com/world/2014/jun/06/egypt-criminalises-sexual-harassment (Accessed 28 July 2014.)

888 National Conference of State Legislatures, "State 'Revenge Porn' Legislation," last updated April 30, 2014, www.ncsl.org/research/telecommunications-and-information-technology/state-revenge-porn-legislation.aspx (May 5, 2014).

889 Geoffrey King. 6 May 2014. The Marco Civil da Internet. Joel Simon (ed). *Halftime for the Brazilian press: Will justice prevail over censorship and violence?* New York, Committee to Protect Journalists, pp. 31–35. https://cpj.org/reports/brazil2014-english.pdf

890 Congressman Alessandro Molon, Rapporteur of the Marco Civil da Internet. Interview with Celina Beatriz Mendes de Almeida. Personal interview. Rio de Janeiro, Brazil, 17 April 2014.

891 Sam Frizell. 7 January 2014. Israel Bans 'Revenge Porn'. *Time*. http://world.time.com/2014/01/07/israel-bans-revenge-porn (Accessed 25 April 2014.)

892 Julian Ryall. 23 January 2014. Japan Plans to Crack Down on 'Revenge Porn' with New Legislation. *South China Morning Post*. www.scmp.com/news/asia/article/1411867/japan-plans-crack-down-revenge-porn-new-legislation (Accessed 3 May 2014.)

893 Daniel Proussalidis. 20 November 2013. Cyberbullies Face 5 Years in Jail Under New Law. *The Toronto Sun*. www.torontosun.com/2013/11/20/cyberbullies-face-5-years-in-jail-under-new-law (Accessed 4 May 2014.)

894 Cyber Civil Rights Initiative. About Us. www.cybercivilrights.org/about (Accessed 24 June 2014.)

895 David Schwartz. 1 May 2014. Arizona Governor Signs Legislation to Discourage 'Revenge Porn'. *Reuters*. www.reuters.com/article/2014/05/01/us-usa-arizona-revengeporn-idUSBREA4000T20140501 (Accessed 5 May 2014.)

896 Article 36 'establishes the right of an injured party to proceed against an ISP that uses the Internet to infringe upon the civil rights and interests of another person, or that is aware that users are utilizing the ISP network to commit a tort and yet fails to take necessary measures (such as deletion, screening or disconnection) or fails to take necessary measures after receiving notice from an injured party and by this failure enlarges the damages.' John V. Grobowski and Yiqiang Li. 1 February 2010. Tort Liability Law of the People's Republic of China. Faegre Baker Daniels LLP. www.faegrebd.com/10911 (Accessed 30 July 2014); Peter Neumann and Calvin Ding. 1 March 2010. China's New Tort Law: Dawn of the Product Liability Era. *China Business Review*. www.chinabusinessreview.com/chinas-new-tort-law-dawn-of-the-product-liability-era (Accessed 30 July 2014); Government of China. 10 January 2010. English Translation of the Tort Law of the People's Republic of China. WIPO. www.wipo.int/wipolex/en/text.jsp?file_id=182630 (Accessed 30 July 2014.)

nude photos of his ex-girlfriend online was sentenced to prison for two years.[897] In July 2010, a Shanghai court ordered Baidu to display, for a period of three days, a public apology to a woman whose ex-boyfriend had disseminated naked photos of her online. Upon losing the case, Baidu assigned 200 employees to 'manually filter and delete related search results'. At a court hearing in October 2009, Baidu stated that it was merely a search engine and that it bore no responsibility for publishing the images.[898]

6.3.2 Policies and practices of intermediaries

Negative media coverage and pressure from civil society groups have prompted some intermediaries to proactively implement mechanisms to prevent and respond to sexual harassment. For example, the social networking services Sina Weibo, Facebook and Twitter prohibit harassment and allow users to report abuse.[899] Responsiveness and enforcement, however, vary depending on the degree of company commitment and attention to the issue, public pressure, and legal enforcement. As elaborated later in this study, in one example of how public pressure has prompted companies to change policies, in the United States the hashtag #FBRape persuaded advertisers to withdraw ads from Facebook, prompting it to take stricter enforcement.[900]

In a 2014 study examining how Facebook, Twitter and YouTube handle violence against women, the Association for Progressive Communication concluded that while company approaches to violence against women differ, and the companies "have made some effort to respond to user concerns," nonetheless "they do not do enough."[901] The study, titled "Internet intermediaries and violence against women online" identified four over-arching themes and trends emerging from their in-depth examination of the three companies.

First, the study found a 'reluctance to engage directly with technology-related violence against women, until it becomes a public relations issue.' Specifically, neither Twitter nor Facebook had taken what APC considered to be 'genuine' or 'concrete' steps to

---

897 Man Who Posted Ex-Girlfriend's Nude Photos Online Was Sentenced To Prison For Two Years. 10 December 2009. *New Express*. http://news.sina.com.cn/s/2009-12-10/015019226383.shtml (Accessed 29 July 2014); Man Who Disseminated Ex-Girlfriend's Nude Photos Committed the Crime to Insult. 14 October 2009. *Yangcheng Evening News*. www.ycwb.com/epaper/ycwb/html/2009-10/14/content_620274.htm (Accessed 29 July 2014.)

898 Peng Pu. 2 July 2010. First sex photo case won in court. *Global Times*. www.globaltimes.cn/content/547661.shtml (Accessed 31 July 2014); Qian Tao. 2011. Intermediary Liability of Website Operators in Privacy Cases in China. *Masaryk University Journal of Law and Technology*, Vol. 5, No. 1, pp. 113–14. http://mujlt.law.muni.cz/storage/1327951355_sb_09-tao.pdf (Accessed 31 July 2014.)

899 Yuki Noguchi. 13 December 2013. Twitter Critics Say It's Not Sensitive Enough To Cyberbullying. NPR 'All Tech Considered'. www.npr.org/blogs/alltechconsidered/2013/12/13/250802010/twitter-critics-say-its-not-sensitive-enough-to-cyberbullying (Accessed 28 July 2014.)

900 Laura Stampler, "Facebook Will Block Photos Celebrating Rape Following Ad Boycott", *Business Insider,* 28 May 2013, accessed 28 July 2014, www.businessinsider.com/facebook-fbrape-ad-boycott-2013-5.

901 Carly Nyst. End violence: Women's rights and safety online project – Internet intermediaries and violence against women online. Executive summary and findings'. Association for Progressive Communications (APC). July 2014. http://www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf

'promote women's rights and specifically address violence against women until public scandals and resulting high-profile campaigns emerged in respect of the intermediary.'[902]

Second, the study identified a "lack of transparency around reporting and redress processes." Specifically:

> The primary challenge encountered by the researchers when conducting this study was the lack of available information about the reporting and redress processes available to victims of technology-related violence. Facebook provides the most information online about its reporting processes, but there remain serious gaps in information about the way complaints are dealt with, and the tests/thresholds applied. Twitter provides very little information about reporting processes but significant information about the circumstances under which it will cooperate with law enforcement; this should be contrasted with YouTube, which provides no information about law enforcement cooperation.[903]

Third, the study found a widespread failure by the three companies "to engage with the perspectives of non-North American/European women." The report points out that "Facebook and Twitter both claim to interact with women's rights groups, but do not appear to have any formal relations with women's rights groups outside of Europe and North America." APC researchers concluded it was impossible to tell 'whether they have an appreciation for international human rights and national legal framewoks regarding violence against women.'[904]

Fourth, the study found that while the companies all make statements in support of free speech, "none of the companies makes a public commitment to human rights standards or to the promotion of rights" and "none of the available policies explicitly address gender-related violence or harassment nor take a strong stance on respect for diversity or for women's rights."[905]

Despite these problems the study did identify several positive developments. Both Twitter and Facebook had 'shown a willingness to opening a diologue with the women's rights community'. All three companies have 'progressively simplified their reporting mechanisms, ensuring that content can be reported at its source.' APC also flagged some proactive steps by Google's YouTube:

> YouTube has been trialling a new system called the YouTube Deputy Program, in which certain users, with a history of accurate reporting of offensive or otherwise inappropriate content, are invited to have more robust flagging tools, allowing them to flag content in bulk. YouTube has started to invite some organisations to trial the system, with the thinking that some groups may have specialised knowledge or expertise that may help them flag. There is a possibility that this system could be opened up to local women's organisations

902 Nyst, op. cit. p.3.
903 Ibid.
904 Nyst, op. cit.p.4.
905 Ibid.

> or the like. This would allow stakeholder groups to take proactive steps to eradicate technology-related violence against women.[906]

The APC report calls on internet intermediaries to balance their commitment to freedom of expression with other human rights 'such as that to be free from discrimination and violence'.

Indeed, it can sometimes be difficult to pinpoint where free expression stops and victimization begins. In June 2014, for example, YouTube drew criticism from the Egyptian Government for refusing to take down a video recording the mass rape of a 19-year-old woman at President Abdel Fattah el-Sisi's inauguration. In response, YouTube said that it 'always remove[s] videos entirely where there is a privacy complaint *and an individual is clearly identifiable*' (emphasis added), noting that in this case the attack's 'newsworthiness' contributed to the company's decision to allow blurred videos concealing the victim's identity. WITNESS, a nonprofit that seeks to use citizen videos documenting abuse to effect change, applauded YouTube's 'nuanced stance'.[907] YouTube also requires users wishing to view the video to vouch they are 18 years old or older.[908]

As the APC report pointed out, sometimes companies come up with mechanisms to report abuse only after being subject to strong public criticism. After stonewalling women's rights advocates when they reported misogynistic pages glorifying date rape and domestic violence,[909] Facebook finally took action. For example, a group called Women, Action and the Media and the Everyday Sexism Project had to send thousands of emails to companies that advertise on Facebook; after Nissan and several smaller companies threatened to withdraw advertising, Facebook finally admitted that its 'systems to identify and remove hate speech have failed to work as effectively as we would like, particularly around issues of gender-based hate'.[910]

At the same time, just as social media platforms are spaces where women or men face sexual and gender-based harassment, social media platforms also enable activists to

---

906 Nyst, op. cit. p.5

907 Madeleine Bair. 25 June 2014. Consent, Privacy, and A Video of Sexual Assault. WITNESS Blog. http://blog.witness.org/2014/06/consent-privacy-video-sexual-assault (Accessed 30 July 2014.)

908 David Clark Scott. 14 June 2014. Why YouTube won't remove Egyptian sexual assault video. *Christian Science Monitor*. www.csmonitor.com/World/Global-News/2014/0614/Why-YouTube-won-t-remove-Egyptian-sexual-assault-video (Accessed 28 July 2014); Lizzie Dearden. 14 June 2014. YouTube refuses Egypt's request to remove footage of Tahrir Square sexual assault. *The Independent*. www.independent.co.uk/news/world/africa/youtube-refuses-egypts-request-to-remove-footage-of-tahrir-square-sexual-assault-9537086.html (Accessed 28 July 2014); Madeleine Bair. 25 June 2014. Consent, Privacy, and A Video of Sexual Assault. *WITNESS* Blog. http://blog.witness.org/2014/06/consent-privacy-video-sexual-assault (Accessed 28 July 2014.)

909 Women, Action and The Media. 27 May 2013. Examples of Gender-Based Hate Speech on Facebook. www.womenactionmedia.org/examples-of-gender-based-hate-speech-on-facebook (Accessed 31 July 2014.)

910 Marne Levine. 28 May 2013. Controversial, Harmful and Hateful Speech on Facebook. Facebook Safety. www.facebook.com/notes/facebook-safety/controversial-harmful-and-hateful-speech-on-facebook/574430655911054 (Accessed 30 July 2014); Tanzina Vega. 29 May 2013. Facebook Says It Failed to Bar Posts With Hate Speech. *New York Times*. www.nytimes.com/2013/05/29/business/media/facebook-says-it-failed-to-stop-misogynous-pages.html (Accessed 30 July 2014.)

fight harassment and raise awareness. In some cases these campaigns have succeeded in bringing national attention to the issues at hand and motivated political and policy-level change. This includes the 2012 campaign in Germany that resulted in a national debate, but which started on Twitter under the hashtag *#aufschrei* (German for 'outcry') through which individuals would tweet about everyday sexism against women.[911] Similarly, in Kenya, the hashtag #SGBVJusticeKE on Twitter seeks to highlight the public interest case where eight survivors of sexual violence during the post-election violence in 2007 have brought a constitutional complaint against the Attorney General and five other senior government officials.[912]

6.4 Conclusion

The previous chapter on social networking platforms found that global companies like Twitter and Facebook are much less transparent and accountable about how they enforce their terms of service than they are about how they handle government requests. The APC study cited in this chapter reinforces the need for greater dialogue and communication with all stakeholders about how social networking platforms develop and enforce their rules. Companies need to work more closely with users, human rights advocates of all kinds (including those advocating for gender rights as well as freedom of expression rights) and governments if the problem of online gender-based violence is to be addressed in a manner that also upholds and protects online freedom of expression.

Indeed, the problem of online gender-based violence underscores the urgent need for a multistakeholder process to develop principles, standards, and 'best practice' guidelines for how social networking platforms should communicate with and listen to users about development and enforcement of their terms of service.

911 Axel Maireder and Stephan Schlögl. 17 February 2014. 24 Hours of an #outcry: The Networked Publics of a Socio-Political Debate. *European Journal of Communication*, Vol. 29, forthcoming, http://homepage.univie.ac.at/axel.maireder/php/wordpress/wp-content/MairederSchloegl_24HoursOfAnOutcry_PrePrint.pdf; Silke Wünsch. 26 January 2013. Anti-sexism Twitter campaign gains momentum. *Deutsche Welle*. www.dw.de/anti-sexism-twitter-campaign-gains-momentum/a-16552842 (Accessed 28 July 2014); Melissa Eddy and Chris Cottrell. 29 January 2013. German Politician's Remark Stirs Outcry Over Sexism. *New York Times*. www.nytimes.com/2013/01/29/world/europe/29iht-germany29.html (Accessed 28 July 2014.)

912 ICJ Kenya. 26 March 2013. Hearing of the PEV Sexual Gender Based Violence case begins in Court. Kenyan Section of the International Commission of Jurists. www.icj-kenya.org/index.php/media-centre/news/596-hearing-of-the-pev-sexual-gender-based-violence-case-begins-in-court (Accessed 31 July 2014.)

7. GENERAL CONCLUSIONS

As an international intergovernmental organization that operates with a global remit and promotes values that are universal, UNESCO has proposed a conceptual framework of Internet "universality."[913] Respect for four core principles is a precondition for the Internet to be universal: (i) human **r**ights; (ii) **o**penness; (iii) **a**ccessibility; and (iv) **multistakeholder** participation. The four can be summarized by the mnemonic R – O – A – M (Rights-based, Open, Accessible, Multistakeholder driven).[914] This report's research findings highlight key challenges for realizing the first principle, human rights.

As discussed in the introductory chapter, this report builds on the UN Guiding Principles for business and human rights, according to which states have a primary duty to protect human rights, businesses have a responsibility to respect human rights, and both spheres have a role in providing remedy to those whose rights are violated.

The case studies in this report highlight the difficulties that internet intermediaries face in maximizing respect for users' right to freedom of expression when states do not uphold their own duty to protect. The cases above highlight ways in which all states have room for improvement. However it is also clear from the case studies that Internet intermediaries have considerable power to influence outcomes affecting internet users' freedom of expression even when the legal and regulatory environment is not fully supportive of that aim.

7.1 State duty to protect

Part of the state's duty to protect human rights includes facilitating and supporting intermediaries' respect for freedom of expression. This report's findings illustrate how, to varying degrees, policies, laws, and regulations are not well aligned with that particular aspect of the state's duty to protect human rights. Issues identified in the case studies included:

1. The characteristics of **intermediary liability regimes** or lack thereof, as well as the regulatory objectives of the regimes (as elaborated in Chapter 2) affect intermediaries' ability to respect freedom of expression. Limiting the liability of intermediaries for content published or transmitted by third parties is essential to the flourishing of internet services that facilitate expression.

913 UNESCO Universality. op. cit.
914 Feedback sought for UNESCO's research on the Internet. UNESCO Communication and Information. 7 March 2014. http://www.unesco.org/new/en/communication-and-information/resources/news-and-in-focus-articles/all-news/news/open_consultation_on_unesco_new_concept_internet_universality

2. Laws, policies, and regulations requiring intermediaries to carry out **content restriction, blocking, and filtering** in many jurisdictions are not sufficiently compatible with international human rights standards for freedom of expression.

3. Laws, policies, and practices related to government **surveillance** and data collection from intermediaries, when insufficiently compatible with human rights norms, impede intermediaries' ability to adequtely protect users' privacy.

4. **Licensing agreements** can affect intermediaries' ability to respect freedom of expression. This applies to ISPs in all countries studied and social networks and search engines in some countries.

5. Whereas due process generally requires that legal enforcement and decision-making are **transparent** and publicly accessible, governments are frequently opaque about requests to companies for content restriction, the handover of user data, and other surveillance requirements. This makes it difficult for the public to hold governments and companies appropriately accountable when users' right to freedom of expression is unduly restricted—either directly, or indirectly through the compromise of user privacy.

7.2 Responsibility of business to respect

Companies' own policies and practices affect Internet users' freedom of expression both positively and negatively. The case studies examined terms of service enforcement, identity policies, transparency practices, the extent to which companies are willing or able to contest government requests, and policies related to privacy, data retention and data protection. Key findings are as follows:

1. **Transparency on content restrictions:** (All three types of intermediaries) Companies studied in this report can offer transparency about how they decide to filter, remove, or otherwise restrict content either in response to requests from governments or third parties, or in the course of enforcing and their own terms of service. Tranparency includes giving notice where content is restricted to those trying to access it, as well as notifying those publishing the content. Companies can offer comprehensive or aggregated overviews of content restriction requests and the company's compliance with them. Despite the recent "transparency reporting" trend by some companies, companies performed inconsistently in terms of what they choose to reveal and how the information is communicated. There is a further lack of transparency by companies about many aspects of their processes, particularly how they enforce terms of service and respond to private requests.

2. **Ability to contest content restriction demands:** Throughout the case studies it became evident that companies may not follow through on all government or other official demands to restrict content. Companies with clear policies and practices on handling content restriction requests are able to contest and minimize the impact

of local laws and regulations that fail to meet international standards for legitimate limitations.

3. **Self-regulation and terms of service enforcement:** Internal decisions agreements among companies - particularly by social media companies - to restrict certain types of content, to enforce of their own private rules, are often welcomed by governments as a way to handle problems before they escalate into matters for the courts and law enforcement. At the same time, these rulemaking and enforcement processes lack transparency or independent oversight mechanisms that would help to ensure that they are not subject to errors and abuses. In summary, the roles may be distinguished as follows:

- *Internet Service Providers:* terms of service for ISPs in all countries studied are specific to each jurisdiction in which they operate and these generally ban illegal activity on their services. Some ISPs in some countries work through self-regulatory frameworks or take instructions from non-governmental bodies to identify illegal content or activity.
- *Search engines:* Of the three search engines studied, the terms of service of Yandex (Russia) and Baidu (China) restrict what is required by law. Only Google (U.S.) restricts substantial categories of content in its terms of service and internal policies extending beyond what is required by law becaues its home jurisdiction has relatively few legal restrictions on expression.
- *Social networking platforms:* Weibo (China) forbids all content that is illegal under Chinese law which itself is broad enough that wide categories of political and religious speech have recently been identified as illegal by Chinese authorities. iWiW (Hungary) forbade content that was also forbidden by the law as well as other categories of content such “vulgar” or “obscene” speech and “overt” or “covert” advertising. The terms of service of Twitter and Facebook (U.S.) both globally restrict (to varying extents) a range of content categories not illegal in the U.S. In certain other jurisdictions they sometimes carry out targeted restriction of content in those jurisdictions where government requests identify the content as infringing.

Governments also use the terms of service abuse reporting mechanisms to flag content which may or may not be illegal, but that violates the companies’ own rules. Also, users in most countries studied reported incidents in which measures were taken against content that did not appear to violate the terms, or in which the terms were enforced in an excessively literal way (e.g., deletion of breastfeeding-promotion pages and pictures) resulting in a negative impact on freedom of expression, and often without adequate means for appeal (see also *Access to remedy* below).

4. **Privacy policies, data retention and data protection:** (Applies to all three types of intermediaries studied here, especially ISPs and social networks) Companies in all three case studies collected similar types of data, although policies about retention and third party sharing differed widely, as did the extent to which companies inform users about whether policies exist and what they are. The majority of companies did

not clearly explain how they handle government requests for user data, nor did they offer information on actual requests for user data or compliance with those requests (the researched social networks stood out more positively in this regard). While law was a contributing factor to some of these differences, differences between the same service type in the same jurisdiction indicate other company-specific factors at play.

5. **Identity policies:** (All three types of intermediaries studied here, especially ISPs and social networks). Whether users are allowed to use a service or create an account without having their account linked to their government-issued identity, or without having to use their real name, impacts users' freedom of expression in many jurisdictions studied.

7.3 Access to remedy

Remedy is the third central pillar of the UN Guiding Principles on Business and Human Rights, placing an obligation on governments and companies to provide individuals access to effective remedy. This area is where both governments and companies have much room for improvement. Across intermediary types, across jurisdictions and across the types of restriction, individuals whose content or publishing access is restricted as well as individuals who wish to access such content had inconsistent, limited, or no effective recourse to appeal restriction decisions, whether in response to government orders, third party requests or in accordance with company policy. While some companies have recently increased efforts to provide appeal and grievance mechanisms and communicate their existence to users, researchers identified examples of rules being inconsistently enforced and enforced in a manner also not consistent with the principles of due process.

7.4 Issues of concern

Company policies and practices can combine with jurisdictional contexts to produce outcomes that have a negative impact on freedom of expression. ***All three case studies identified several common categories of issues:***

- **Necessity and proportionality in content restriction:** Over-broad law and heavy liability regimes cause intermediaries to over-comply with government requests in ways that compromise users' right to freedom of expression, or broadly restrict content in anticipation of government demands, even if demands are never received and if the content could potentially be found legitimate even in a domestic court of law.
- **The Internet's transnational nature places particular limits on the operating space for intermediaries:** Intermediaries can be subject to different legal norms, and are sometimes at risk of an all-out ban by authorities disagreeing with particular content shared via the services. Internet services at times resist such pressures by

closer cooperation with governments or sometimes by blocking content only in the jurisdiction in question, or sometimes by wholescale deletion of said content.

- **Variety of actors involved creates uncertainty about permitted content:** Companies decide to allow or ban certain content based on their internal policies, as well as being influenced by legal obligations following court rulings, governmental orders, civil claims, instructions by third parties, monitoring groups with which the intermediary cooperates, and others. This myriad of actors involved, compounded by ambiguity of legal frameworks, often makes it unclear for individual users what content is permitted, who decides on allowed content, and how, and the potential consequences of their expression.
- **Gender Issues:** The existence and nature of company policies dealing with speech related to sexual harassment, gender-based violence and exploitation or objectification of women are uneven, even across the same intermediary type and jurisdiction. Companies in all three case studies had in place mechanisms allowing users to report abuse. These mechanisms could be used for legitimate purposes, including reporting sexual harassment, but at the same time some stakeholders expressed concerns that the same mechanisms could also be used to abuse users' legitimate freedom of expression rights.

7.5 Intermediaries and Internet Governance

In 2005, the UN Working Group on Internet Governance (WGIG) defined "Internet governance" as "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet."[915] Thus while the term "Internet governance" is often used in the media and public debates in a narrow sense to describe the technical policymaking and coordination functions of organizations such as the International Corporation for Assigned Names and Numbers (ICANN), the concept was originally conceived to encompass a broader set of processes for determining policies and practices that shape the Internet's functioning at all layers.

The policy role of internet intermediaries – and policies affecting their operations – is a form of Internet governance broadly defined.[916] It is therefore useful to situate this report's findings in the context of global debates over core principles for internet policymaking that have a direct impact on intermediaries.

The annual Internet Governance forum (IGF), whose creation was mandated by the 2005 Tunis Agenda for the Information Society, provides a platform for stakeholders to debate the full range of issues surrounding the Internet's governance, albeit without a

915 Report of the Working Group on Internet Governance. Château de Bossey. June 2015. http://www.wgig.org/docs/WGIGREPORT.pdf

916 Laura DeNardis. August 2013. Internet Points of Control as Global Governance. Internet Governance Papers. No.2. Centre for International Governance Innovation. http://www.cigionline.org/sites/default/files/no2_3.pdf

mandate to set policy.[917] A number "dynamic coalitions" were formed to support on-going work related to a range of concerns related to the information society[918] leading to the emergence in 2008 of the multistakeholder Internet Rights and Principles (IRP) Dynamic Coalition.[919] The IRP developed a Charter of Human Rights and Principles for the Internet,[920] with a set of ten core principles launched in 2011 including principles on freedom of expression and privacy.[921] Notably, this development work preceded the release of the first report by UN Special Rapporteur on freedom of expression Frank La Rue in 2011 and the Human Rights Council's first resolution on the Internet and human rights in 2012, the content of which was discussed in greater detail at the beginning of this report's introductory chapter.

In February 2014 the European Commission submitted a report to the European Parliament on Internet policy and governance, proposing an approach to developing principles for global Internet policy and governance. This approach built on the Tunis agenda of 2005 and is represented by the acronym, COMPACT: "the Internet as a space of **C**ivic responsibilities, **O**ne unfragmented resource governed via a **M**ultistakeholder approach to **P**romote democracy and human rights, based on a sound technological **A**rchitecture that engenders **C**onfidence and facilitates a **T**ransparent governance both of the underlying Internet infrastructure and of the services which run on top of it".[922] Since Tunis, the document states, "there has been a proliferation of Internet governance principles in various fora but in most cases each one supported by a limited set of stakeholders, or limited in geographical scope." The COMPACT principles, the Commission argued, have the potential to support "a process leading towards a more broadly supported and coherent set of principles for Internet governance [that] would be helpful in finding common ground."[923]

In April 2014 the Brazilian government convened an international multistakeholder conference called "NETmundial" to discuss "Internet governance principles" and a "roadmap for the future evolution of the Internet Governance system."[924] Negotiations among governments, industry, civil society and the technical community produced a "multistakeholder statement" whose commitments on free expression and privacy principles went beyond previous commitments agreed by UN member states at the World

---

917 APC Internet Rights Charter. last updated November 2006. http://www.apc.org/en/node/5677/.

918 Wolfgang Benedek, Veronika Bauer, and Matthias C. Ketteman eds., *Internet Governance and the Information Society: Global Perspectives and European Dimensions,* (Utrecht: Eleven International Publishing, 2008), p. 37.

919 The IRP coalition. Internet Rights & Principles Coalition website. http://internetrightsandprinciples.org/site/about/.

920 Internet Rights & Principles Charter. http://internetrightsandprinciples.org/wpcharter/.

921 IRP campaigns: 10 Internet Rights & Principles. http://internetrightsandprinciples.org/site/campaign/.

922 Internet Policy and Governance Europe's role in shaping the future of Internet Governance. 12 February 2014. The European Commission. COM(2014) 72 final. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2014:0072:FIN:EN:PDF

923 Ibid. p.4

924 Dilma Rousseff. 23 April 2014. Opening Speech. NETmundial. http://netmundial.br/wp-content/uploads/2014/04/NETMundial-23April2014-Dilma-Rousseff-Opening-Speech-en.pdf and NETmundial Multistakeholder Statement. 24 April 2014. http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Summit on the Information Society (WSIS) in Tunis in 2015.[925] Notably, its clauses on freedom of expression, association and access to information reinforced the emerging international consensus – discussed in detail in this report's introductory chapter – that offline rights should be equally protected online. There was much less consensus around sections relating to intermediary liability and online privacy. As the case study findings of this report highlight, even if there appears to be stronger general consensus about the principle of freedom of expression, governments and companies still have a long way to go when it comes to translating such consensus into actual practice.

The September 2014 IGF in Istanbul saw the launch of a new Dynamic Coalition on "Platform Responsibility" focusing on a specific category of intermediaries, "social networks and other interactive online services," to discuss "concrete and interoperable solutions to protect platform-users' human rights."[926] This new Dynamic Coalition has similar potential to contribute to stronger norms for social networking services, search engines and other types of intermediaries that can be defined as 'platforms' for expression. There is a particular opportunity for this dynamic coalition to serve as a focal point for developing stronger human rights-based principles and accountability mechanisms for various emerging forms of self- and co- regulation.

The following recommendations are offered by this report's authors in the spirit of principles such as UNESCO's ROAM formula, and the EC's COMPACT and Netmundial, in the hopes of fostering further discussion and eventually building greater international consensus around best practices by all stakeholders.

925 Tunis Commitment. Second Phase of the WSIS (16-18 November 2005, Tunis) WSIS-05/TUNIS/DOC/7. http://www.itu.int/wsis/documents/doc_multi.asp?id=2266%7C0. Also see Milton Mueler. 27 April, 2014. Netmundial Moves Net Governance Beyond WSIS. Internet Governance Project blog. http://www.internetgovernance.org/2014/04/27/netmundial-moves-net-governance-beyond-wsis/ (Accessed May 6, 2014.) and David Johnson. The Unanswered Questions of Netmundial. Internet Governance Project Blog. 30 April 2014. http://www.internetgovernance.org/2014/04/30/the-unanswered-questions-of-netmundial/ (Accessed 6 May, 2014.)

926 Dynamic Coalition on Platform Responsibility. 'About' page. http://platformresponsibility.info/?page_id=2

8. RECOMMENDATIONS

The following recommendations apply in varying degrees to all stakeholders: governments, companies, civil society and multinational organizations. If online freedom of expression is to be adequately respected and protected, all of these actors must find ways to work together across borders to improve legal and regulatory frameworks, establish and implement corporate best practices, and increase awareness as well as participation by internet users and citizens. Rulemaking and enforcement related to online speech – whether carried out by governments or companies – must be compatible with and held accountable to international human rights norms. The recommendations below are offered as first steps in that direction.

1. Adequate legal frameworks and policies.

Policy, legal, and regulatory goals affecting intermediaries must be consistent with universal human rights norms if states are to protect online freedom of expression and if companies are to respect it to the maximum degree possible. Governments need to ensure that legal frameworks and policies are in place to address issues arising out of intermediary liability and absence of liability. Legal frameworks and policies affecting freedom of expression and privacy should be contextually adapted without transgressing universal standards, be consistent with human rights norms including the right to freedom of expression, and contain a commitment to principles of due process and fairness. Legal and regulatory frameworks should also be precise and grounded in a clear understanding of the technology they are meant to address, removing legal uncertainty that would otherwise provide opportunity for abuse or for intermediaries to operate in ways that restrict freedom of expression for fear of liability.

In order to better inform public and private policymaking processes, there is a need for much more qualitative and quantitative global research on the impact of company policies, practices, business models, and design choices on freedom of expression. Comprehensive surveys of internet users around the world on how intermediaries affect individuals' freedom of expression in different contexts are currently lacking. More research is also needed on how legal, regulatory and policy frameworks affect intermediaries' ability to respect users' rights, as well as their impact on Internet users more broadly. This study only begins to scratch the surface in its examination of how specific companies' policies and practices affect freedom of expression in different jurisdictions. More detailed facts about cause-and-effect between policies, practices and outcomes are needed. These facts will better equip all stakeholders to refine and adjust their policies, practices, and strategies to maximize the protection of and respect for freedom of expression rights of Internet users everywhere in the world.

2. Multistakeholder policy development.

Laws, regulations and **governmental** policies, as well as **corporate** policies, are more likely to be compatible with freedom of expression if they are developed in consultation with all affected stakeholders – particularly those whose rights are known to be at risk – and take into account those interests. A genuine multistakeholder process involves all stakeholders potentially affected by the policy from the start, rather than simply seeking opinions after the basic parameters have been set and key directions already determined.

3. Transparency.

Transparency is important to demonstrate that governance and enforcement actions are in compliance pre-specified principles, rules and conditions.

Greater transparency **by governments** about requests and requirements being placed on companies that have the potential to affect Internet users' freedom of expression and privacy is a prerequisite for accountability in public governance of the Internet.

Transparency **by companies** is a prerequisite for accountability in how intermediaries respond to government requests, as well as their own private "governance," which in turn is necessary not only for the protection of Internet users' freedom of expression, but for companies ability to earn and maintain public trust in their services.

In this context there are two kinds of transparency: qualitative and quantitative. Qualitative transparency involves governments making publicly available, the laws, legal interpretations, administrative procedures and other measures related to content restriction and surveillance. For companies, qualitative transparency involves communicating with users about processes for responding to government requests and for enforcing internal company rules and processes. Quantitative transparency refers to the publication of aggregate data about government requests and compliance rates, as well as other data that helps internet users understand what types of content are being removed under what auspices for what reason.

The GNI and Center for Democracy and Technology have developed the following transparency recommendations for governments regarding content restriction:

- Publicly post laws authorizing orders to remove or restrict content as well as official legal interpretations of the law, including executive orders, legal opinions that are relied on by executive officials, and court orders.
- Disclose the information about:
    - Which government agencies/bodies are legally permitted to order takedowns;
    - The types of information by subject that can be ordered removed;
    - The judicial, ministerial, or other oversight mechanisms required for the authorization of each instance of content removal;

- The judicial, ministerial, or independent oversight mechanisms that oversee the implementation of content takedowns;
- The mechanisms for redress that victims of unlawful censorship may pursue;
- Public disclosure of the scope of unlawful censorship and remedial and disciplinary actions taken.

- Permit companies to disclose the number of takedowns requests that they receive by number, subject matter, and specific legal authority, and how the company responded to the request.[927]

Similar transparency measures are recommended for governments in reporting both qualitatively and quantitatively on surveillance. Companies should disclose aggregated information on the number of user data and real-time surveillance requests that they receive, and how the company responds to them, on at least an annual basis. Governments should enact legal reforms that clearly permits such transparency. Companies should also be able to disclose the existence and basic details about any technical requirements for surveillance that governments impose upon them.

4. Privacy.

Protecting users' right to privacy is essential for freedom to expression to flourish. **Intermediaries** should adopt best practices with respect to privacy. Intermediaries must also have clear and comprehensible policies in place for what information about users they collect and store, how they handle it, with whom they share it, and under what circumstances authorities may obtain access to such data. Such policies must be prominent and easy to access.

For **governments**, policies, regulations laws, and enforcement practices affecting Internet users' privacy, including data collection and surveillance for law enforcement purposes, should be consistent with core human rights principles outlined in this report's first recommendation. The 'International Principles on the Application of Human Rights to Communications Surveillance' developed by a global coalition of civil society groups between late 2012 and May 2014, set forth 13 concrete principles that governments and companies should follow to ensure that communications surveillance is carried out in a manner consistent with international human rights standards.[928]

927 Susan Morgan and Emma Llansó. Letter to Members of the Freedom Online Coalition Working Group on Privacy and Transparency Online. 29 August 2014.
928 https://en.necessaryandproportionate.org/text

5. Human rights impact assessment.

Protection of online freedom of expression will be strengthened if **governments** carry out human rights impact assessments to determine how proposed laws, regulations or policies may affect Internet users' freedom of expression and/or privacy domestically and globally, and publish the results of those assessments.[929]

Companies should also carry out human rights impact assessments to determine how their policies, practices, and business operations affect Internet users' freedom of expression and adapt their activities accordingly with strategies to mitigate potential harms identified in the assessments.[930] Such assessment processes should be anchored in robust engagement with stakeholders whose freedom of expression rights are at greatest risk online or those who are able to able to represent those interests, as well as stakeholders who harbor concerns about other human rights affected by online speech. Strategies to mitigate negative impact on freedom of expression can include, for example:

a. the training of staff to enable informed decision-making on content restrictions based on clear and consistent criteria and process;

b. the development of a "rapid human rights impact assessment" process in specific circumstances when time-sensitive business decisions are being made;

c. creation of informed networks of knowledgeable stakeholders to engage with at key moments.[931]

6. Self-regulation must follow principles of due process and accountability, and be consistent with human rights norms.

National laws need to strengthen due process and the adherence to international human rights norms to protect the rights of Internet users needs, but they are also essential for intermediaries' legitimacy as custodians of online content and should be a guiding principle of private terms of service enforcement processes. This aligns with international standards that require any limitations on free expression to be specified in rule, as distinct from being arbitrary or retroactive. Self-regulation should further respect the principles of necessity, proportionality, and internationally agreed legitimate purpose. Within the

---

929 See Eduardo Bertoni. Internet Regulation and the Need for "Human Rights Impact Assessments" (HRIA) - a Proposal for Debate in Latin America. E-Bertoni. 27 July 2012. http://ebertoni.blogspot.com/2012/07/internet-regulation-and-need-for-human.html (Accessed September 17, 2014.)

930 For more information about human rights impact assessments see: Faris Natour and Jessica Davis Pluess. Conducting an Effective Human Rights Impact Assessment. March 2013. http://www.bsr.org/reports/BSR_Human_Rights_Impact_Assessments.pdf and Michael **A. Samway. Business, Human Rights and the Internet: A Framework for Implementation. in** *Human Dignity and the Future of Global Institutions***. (eds. Arend and Lagon, Georgetown University Press, 2014) pp. 309-312.**

931 Legitimate and Meaningful Stakeholder Engagement in Human Rights Due Diligence: Challenges and Solutions for ICT Companies. BSR, with CDT. September 2014. http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf

context of creating a safe user experience, content restrictions deployed by intermediaries should not only be as minimal as possible, but should also avoid conflict with the key human rights principle of non-discrimination.

In order to identify and mitigate potential adverse impacts on users' freedom of expression, intermediaries should carry out human rights impact assessments on their terms of service and related enforcement policies and practices.

The Internet Society has proposed a set of principles and recommendations for self-regulatory processes and institutions. Key recommendations include specific ways in which self-regulatory mechanisms should build accountantable and transparent practices. Balanced and proportionate rules, due process, and judicial safeguards are all essential. Periodic reviews should also be built into such systems: 'All systems, including public ones, should be periodically reviewed and evaluated as to their effectiveness. Such reviews test the efficacy of policy mechanisms and their ability to provide answers to the issues they were originally created to address.'[932] This is sound advice for traditional regulation as well as companies' private rules and enforcement processes.

7. Remedy.

Internet users have the right to effective remedy when their rights are restricted or violated by intermediaries, by states, or by a combination of the two. It should be possible for people to report grievances and obtain remedy from private intermediaries as well as from government authorities, including national-level human rights institutions. In seeking remedy for restriction or violation of the right to online freedom of expression, Internet users should not necessarily be required to pursue legal action through the courts. Avenues for seeking remedies should be publicly available, known, accessible, affordable and capable of providing appropriate redress.[933]

Depending on national context, grievance and remedy mechanisms provided by **states** may include redress mechanisms such as those provided by data protection authorities, national human rights institutions (such as ombudspersons), court procedures, and hotlines.[934]

Depending on the jurisdictional and operational context, grievance and remedy mechanisms provided by **private intermediaries** (and private regulatory schemes that they may participate in) should provide mechanisms to receive and respond to grievances from Internet users. These should be accessible, secure, and linguistically and culturally-appropriate. The question of whether meaningful remedy is available to users whose freedom of expression rights have been restricted or violated should

---

932 Voluntary Initiatives as a source of policy-making on the Internet. 29 July 2014. The Internet Society. http://www.internetsociety.org/blog/2013/07/voluntary-initiatives-source-policy-making-internet

933 Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users. *(Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies).* Council of Europe. p.4 https://wcd.coe.int/ViewDoc.jsp?id=2184807

934 Ibid. p.1

be examined as part of a company's human rights impact assessment process. Depending on the grievance and the harm identified, remedy might could (but need not necessarily) involve financial compensation. Meaningful remedy measures can also include acknowledgment, apology, and commitment to address the problem in the future; submitting to independent investigation or ongoing oversight; or participation in regional or sector-wide multistakeholder entities to clarify and mitigate potential restriction or violation of users' rights.[935]

8. Public education and information, and media and information literacy.

The composite concept of Media and Information Literacy covers the range of competencies that citizens need for full participation in knowledge societies. In their engagement with internet intermediaries, citizens require a range of of literacies concerning free expression issues. Companies and governments have a role to play in promoting these literacies formally and informally.

States have an obligation to provide accessible and clear information to the public so that Internet users can not only understand and effectively exercise their rights, but also recognize when their rights have been restricted, violated, or otherwise interfered with. State restrictions on freedom of expression must not only pursue a legitimate aim and comply with human rights law, but should also be made clearly known to the public.[936] Public information should also include concrete instructions on official grievance and remedy mechanisms.[937]

Respect of Internet users' rights by private intermediaries also requires informing and communicating with users about their rights as users of the service, how users' expression can be restricted according to the intermediary's terms of service, the reasons for those restrictions and why they are necessary, and other information necessary for a user to make an informed decision about whether or not to use the service.[938]

Educational institutions should be encouraged and incentivized to include information about the rights of Internet users in curricula related to human rights, civics and government. Media should similarly be encouraged and incentivized to include reporting and programming that helps to foster informed public discussion about the rights of Internet users, and the obligations of states and businesses to protect and respect those rights.

935 Telco Remedy Plan. Access. pp 8-10. https://www.accessnow.org/telco-remedy-plan
936 Council of Europe, op. cit. p.3
937 Ibid. p.1
938 Ibid. p.3

9. Global accountability mechanisms

It is important that companies and governments alike make commitments to implement core principles of freedom of expression and privacy. In today's globally networked digital environment, these principles must be implemented in a manner that is accountable locally as well as globally.

Examples from the consumer privacy context include: the European Union's Binding Corporate Rules[939] and the APEC Cross Border Privacy Rules system.[940] Another approach to accountability for companies is through assessment and certification by independent multistakeholder organizations. The Global Network Initiative, a multistakeholder coalition, requires its members to undergo periodic assessments as part of an accountability mechanism for adherence to its principles and implementation guidelines focused on how companies handle government requests. (As noted in this report's introduction, of the companies studied for this report, Google and Facebook are GNI members. Vodafone and Telefonica, the parent company of Vivo, are members of the Telecommunication Industry Dialogue, which works closely with GNI on developing best practice for the telecommunications industry.) The GNI's implementation guidelines and assessment do not currently include consumer privacy issues or terms of service enforcement, however. Other organizations and mechanisms may need to be developed to improve accountability and transparency in these areas if GNI is unable to include them in future.

As for states, a coalition of 23 governments have joined the Freedom Online Coalition, in which member nations agree to work together to advance 'free expression, association, assembly, and privacy online – worldwide.'[941] In April 2014 the coalition's members issued the 'Tallinn Declaration', a set of 'Recommendations for Freedom Online.' [942] Among those recommendations three are particularly relevant to this report:

- Dedicate ourselves, in conducting our own activities, to respect our human rights obligations, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency, and call upon others to do the same,
- Reaffirm support for an open and interoperable internet, noting that strong cyber security and secure and stable communication are critical to maintaining confidence and trust in the internet, and key to safeguarding human rights and realising the internet's economic, social and cultural benefits,
- Call upon governments worldwide to promote transparency and independent, effective domestic oversight related to electronic surveillance, use of content take-

939 Overview on Binding Corporate Rules. Data Protection. European Commission. http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm
940 APEC Cross-Border Privacy Rules System http://www.cbprs.org/
941 Freedom Online Coalition. https://www.freedomonlinecoalition.com/
942 Recommendations for Freedom Online. Adopted in Tallinn, Estonia on April 28, 2014 by Ministers of the Freedom Online Coalition. https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf

down notices, limitations or restrictions on online content or user access and other similar measures, while committing ourselves to do the same,

Three multi-stakeholder working groups have been set up. The coalition holds an annual conference to which representatives from companies and civil society are invited. However it remains to be seen whether any mechanisms will emerge through which governments can be benchmarked and held accountable by gobal stakeholders on the extent to which they have lived up to the above recommendations. Internet intermediaries will be hard pressed to fully live up to their responsibility to respect human rights unless governments fulfill their own duty to protect human rights including freedom of expression and privacy online.

This study has been focused on three types of Internet intermediaries, assessing their role in fostering freedom of expression. The research is not intended to be a representative or static sample of actors, but rather to extrapolate more general insights. Its aim has been to assist all stakeholders, and not least the intermediaries themselves, to identify how, through the gatekeeping capacity inherent in mediating Internet content can be optimised for freedom of expression and the right to privacy. In this way, internet intermediaries and the companies that operate them can contribute to the evolution of what UNESCO calls knowledge societies, which in turn are central to building democracy, sustainable development and peace around the world.

Acknowledgments

The authors are grateful for the support of Xianhong Hu and Guy Berger of UNESCO, and for the funding support and editorial input by the Internet Society and Open Society Foundations. Furthermore, this report would not have been possible without the editorial and institutional support of Monroe Price, Director of the Center for Gobal Communication Studies at the University of Pennsylvania, and his colleagues Briar Smith, Drew Cahan, and Laura Schwartz-Henderson.

We are also indebted to the John D. and Catherine T. MacArthur Foundation for its support for the Ranking Digital Rights project, based at the New America Foundation, whose research led the research and writing of this report.

Finally, the authors are grateful to members of the report's international advisory committee who provided invaluable input at varying stages of this project:

- Renata Avila, World Wide Web Foundation and Global Voices
- Rasha Abdulla, Associate Professor and Past Chair, Journalism and Mass Communication, The American University in Cairo
- Sunil Abraham, Executive Director, Centre for Internet and Society, Bangalore
- Peng Hwa Ang, Professor, Nanyang Technological University, Wee Kim Wee School of Communication, Singapore
- Eduardo Bertoni: Director of the Center for Studies on Freedom of Expression and Access to Information (CELE) at Palermo University School of Law, Argentina
- Seeta Peña Gangadharan, New America's Open Technology Institute
- Leslie Harris, Principal, Harris Strategy Group LLC; former President and CEO, Center for Democracy and Technology
- Dunstan Allison Hope: Managing Director, Advisory Services, BSR
- Rikke Frank Jørgensen: Senior Advisor, Danish Institute for Human Rights
- Jeremy Malcolm, Senior Global Policy Analyst, Electronic Frontier Foundation
- Pranesh Prakash, Policy Director, Centre for Internet and Society, Bangalore
- Lucy Purdon, Institute for Human Rights and Business
- David Sullivan, Policy and Communications Director, Global Network Initiative
- Ben Wagner, Centre for Internet & Human Rights, European University Viadrina

Glossary

Algorithm: 'A set of ordered steps for solving a problem, such as a mathematical formula or the instructions in a program.'[943]

Anonymity: The ability to 'access and impart information, and to communicate securely, without having to be identified.'[944]

Bandwidth: 'The transmission capacity of an electronic pathway such as a communications line, computer bus or computer channel. Digital bandwidth is the number of pulses per second measured in bits per second (bps). For example, Ethernet transmits at different speeds, including 10 Mbps [Megabits per second], 100 Mbps and 1000 Mbps'[945]

Blog: 'A website, usually maintained by a person with regular entries of commentary, descriptions of happenings, graphics or video. The ability of readers to leave comments in an interactive format is an important part of many blogs.'[946]

Cloud computing: '[A] way of delivering applications, services or content remotely to end users, rather than requiring them to hold data, software or applications on their own devices.'[947]

Content: 'On the Internet, content is any information that is available for retrieval by the user, including Web pages, images, music, audio, white papers, driver and software downloads as well as training, educational and reference materials.'[948]

Cookie: 'A small text file (up to 4KB) created by a Web site you visit that is stored on your computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the Web site to recognize you and keep track of your preferences.'[949]

Data Packet: "[A] unit of data made into a single package that travels along a given network path. Data packets are used in Internet Protocol (IP) transmissions for data that navigates the Web, and in other kinds of networks.'[950]

---

943 'Definition of: algorithm'. *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/37649/algorithm (Accessed 24 October 2014.)
944 Frank La Rue. 17 April 2013. (A/HRC/23/40) Op. Cit. p. 13.
945 'Definition of: bandwidth'. *PC Magazine* Encyclopedia, http://www.pcmag.com/encyclopedia/term/38401/bandwidth (Accessed 25 October 2014.)
946 William H. Dutton, Anna Dopatka, Michael Hills, Ginette Law and Victoria Nash. 2011. *Op Cit.* p. 82.
947 UNCTAD. 2013. *Information Economy Report 2013: The Cloud Economy and Developing Countries*. Switzerland, UN Publications, p. 4. http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf
948 'Definition of: content'. PC Magazine Encyclopedia. http://www.pcmag.com/encyclopedia/term/40264/content (Accessed 25 October 2014.)
949 'Definition of: cookie'. *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/40334/cookie (Accessed 24 October 2014.)
950 'Data Packet'. *Techopedia* Dictionary. http://www.techopedia.com/definition/6751/data-packet (Accessed 24 October 2014.)

Data Protection: Standards that 'place conditions on the collection, use and storage of personal data (rules governing data controllers), give certain rights to the individuals to whom the data relates (data subjects), and provide for a system of oversight to ensure respect for the rules and to address breaches.'[951]

Deep Packet Inspection (DPI): 'A technology which permits access providers to open each "packet" of Internet data sent or received on its network in order to assess where it is coming from, who it is going to and the nature of the file, if it is not encrypted.'[952]

Domain Name: '[A]n Internet resource name that is universally understood by Web servers and online organizations and provides all pertinent destination information. To access an organization's Web-based services, website users must know the precise domain name.'[953]

Email: A portmanteau of '**e**lectronic **mail**' referring to the 'transmission of text messages from sender to recipient…Users can send a mail message to a single recipient or to multiple users' and can attach and transmit computer files in the message.[954]

Encryption: 'A process that takes a message and makes it unreadable except to a person who knows how to "decrypt" it back into a readable form.'[955]

Hashtag: 'A means of providing a common topic identifier in text and chat messages so they can be searched as a group. Commonly used in tweets, the hashtag uses a number sign (#) prefix followed by text. Hashtags can be created and used to identify anything, including people, businesses, organizations, sports teams, political parties, hobbies, events, philosophies, moods, rants and raves.'[956]

Internet: '[A] large network made up of smaller networks…The global Internet comprises nearly a billion Web, e-mail and related servers in more than 100 countries. Originally developed for the U.S. military, it became widely used for academic and commercial research, with access to unpublished data and journals on many subjects. Today, the "Net" is the world's largest source of information on every subject known to humankind.'[957]

Internet filtering: 'A government, an ISP [Internet Service Provider], a company or a parent can install software, either on a personal computer at home or on a server in an organization, that restricts content to users. A filter can screen particular words, e-mail

---

951 Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin, and Natalia Torres. 2012. *Op. Cit.* p. 64.
952 Joe McNamee. January 2011. Op Cit. p. 3.
953 'Domain Name'. *Techopedia* Dictionary. http://www.techopedia.com/definition/1327/domain-name (Accessed 25 October 2014.)
954 "Definition of: e-mail'. *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/42233/e-mail (Accessed 25 October 2014.)
955 'Encryption'. Electronic Frontier Foundation, Surveillance Self-Defense project. https://ssd.eff.org/en/glossary/encryption (Accessed 24 October 2014).
956 'Definition of: hashtag'. *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/60984/hashtag (Accessed 25 October 2014.)
957 'Definition of: internet". *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/45184/internet (Accessed 25 October 2014.)

addresses, Web sites or other addresses and be used for example, if a country wishes to prevent users within its borders from seeing a particular news site online.'[958]

IP address: 'Each device connected to the Internet has a unique number [called an IP address] that allows it to communicate with other devices.'[959] When a device connects with a Web site or online server, its IP address is usually visible. It is possible to determine information such as approximate location or ISP using an IP address.[960]

KB: Acronym for Kilobyte, a measurement of data. One KB equals 1,024 bytes. Text-based files, such as emails or documents, consist of thousands of bytes and are often measured in KB. Audio, image, and video files are much larger and contain millions of bytes. They are measured in MB (Megabytes, or about one million bytes).[961]

Keyword: 'A word used in a text search.' Also, a 'word in a text document that is used in an index to best describe the contents of the document.[962] Filtering software often uses keywords to determine what content or websites to block.

Malware: A combination of '**mal**icious soft**ware**' referring to '[s]oftware 'designed to damage computers or computer systems, such as by installing a computer virus.' [963]

Metadata: (also known as "data about data") and includes 'everything about a piece of information, apart from the information itself. So the content of a message is not metadata, but who sent it, when, where from, and to whom, are all examples of metadata…[M]etadata can often reveal a great deal, and will often need to be protected as carefully as the data it describes.'[964]

MMS: An acronym for **M**ultimedia **M**essaging **S**ervice, MMS is an 'enhancement to the SMS text messaging service that enables images, audio and video files to be transmitted with the text message to a cellphone.'[965]

Net Neutrality: The principle that ISPs should treat all data equally and not prioritize data or services for any reason – including commercial and political ones.[966]

---

958 William H. Dutton, Anna Dopatka, Michael Hills, Ginette Law and Victoria Nash. 2011. Op. Cit, p. 84.
959 Joe McNamee. January 2011. Op. Cit. p. 3.
960 'IP Address'. *Electronic Frontier Foundation*, Surveillance Self Defense project. https://ssd.eff.org/en/glossary/ip-address (Accessed 24 October 2014.)
961 'What units of measurement are used for data storage?' TechTerms.com Help Center. http://www.techterms.com/help/data_storage_units_of_measurement (Accessed 26 October 2014.); 'Kilobytes Megabytes Gigabytes'. CS101, Stanford University. https://web.stanford.edu/class/cs101/bits-gigabytes.html
962 'Definition of: keyword". *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/45808/keyword (Accessed 25 October 2014.)
963 William H. Dutton, Anna Dopatka, Michael Hills, Ginette Law and Victoria Nash. 2011. *Op. Cit.* p. 84.
964 'Metadata'. *Electronic Frontier Foundation*, Surveillance Self Defense project. https://ssd.eff.org/en/glossary/metadata (Accessed 24 October 2014.)
965 'Definition of: MMS'. *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/47123/mms (Accessed 25 October 2014.)
966 Barbara van Schewick. 6 May 2014. The Case for Rebooting the Network-Neutrality Debate. The Atlantic. http://www.theatlantic.com/technology/archive/2014/05/the-case-for-rebooting-the-network-neutrality-debate/361809/ (Accessed 24 October 2014.)

Network Level: When telecommunications access providers or ISPs perform a given action, that action occurs at the network level. These actions may not change what content is available on the World Wide Web, but they affect what users can access online. Network-level actions that can restrict free expression include filtering, shutting down service, or deliberately slowing service.

Portal: '[A]ny commonly used website serving as an entry point to the Internet, usually with many links to a wide variety of information, data, resources and services.'[967]

Post: 'To place an entry on a blog or social networking site or to place a new or revised page on a Web site.'[968] An entry on a blog or social networking site is also called a post.

Platform Level: When applications such as search engines, social network sites, or web hosting providers perform a given action, that action occurs at the platform level. These actions can affect what content is available online as well as what content users can access. Platform-level actions that can restrict free expression include deleting content, blocking content from view, or deactivating user accounts.

Pseudonym: '[A] name used in place of one's given (or "real") name. Examples of pseudonyms in the computer world include usernames and handles, which are frequently used when accessing websites or posting comments. A pseudonym may also be known as a false name.'[969]

Search engine optimization: 'Designing a Web site so that search engines find the pages easily and index them. The goal is to have a page rank as high up on the results list as possible...Search engine optimization (SEO) includes the choice of keywords used in the text paragraphs and the placement of those words on the page, both visible and hidden inside meta tags.'[970]

SMS: An acronym for **S**hort **M**essaging **S**ervice, SMS is the 'common text messaging service available on cellphones and other handheld devices.'[971]

SIM Card: Short for subscriber identity module card, a SIM card 'is a portable memory chip used in GSM [Global Standard for Mobiles] phones. It is a crucial component in mobile telecommunications as it identifies and stores the telephone number and connects the cellphone to the mobile carrier's network."[972]

---

967 'Portal (Internet)'. *Techopedia* Dictionary. http://www.techopedia.com/definition/13077/portal-internet (Accessed 25 October 2014.)

968 'Definition of: Post'. *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/49542/post (Accessed 25 October 2014.)

969 'Pseudyonym (nym)'. *Techopedia* Dictionary. http://www.techopedia.com/definition/1707/pseudonym-nym (Accessed 25 October 2014.)

970 'Definition of: search engine optimization'. *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/50995/search-engine-optimization (Accessed 25 October 2014.)

971 'Definition of: SMS'. *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/51563/sms (Accessed 25 October 2014.)

972 'Subscriber Identity Module Card (SIM Card).' *Techopedia* Dictionary. http://www.techopedia.com/definition/23747/subscriber-identity-module-card-sim-card (Accessed 25 October 2014.)

Social media: '[A] catch-all term for a variety of Internet applications that allow users to create content and interact with each other. This interaction can take many forms, but some common types include:

- Sharing links to interesting content produced by third parties
- Public updates to a profile, including information on current activities and even location data
- Sharing photos, videos and posts
- Commenting on the photos, posts, updates, videos and links shared by others'[973]

Spam: Unsolicited and bulk communications. Most spam is in the form of email, but it can also be posted to online chat rooms, message boards, and comments sections. Spam's costs come from the cost to human attention and the large amount of network bandwidth it consumes.

Spider: 'Also known as a "crawler," "robot" (bot) and "intelligent agent," a spider is a program that searches for information on the Web. Spiders are widely used by Web search engines to index all the pages on a site by following the links from page to page. The search engine summarizes the content and adds the links to [its index]. Spiders are also used to locate Web pages that sell a particular product or to find blogs that have opinions about a product.'[974]

Telecommunications: '[T]he exchange of information by electronic and electrical means over a significant distance. A complete telecommunication arrangement is made up of two or more stations equipped with transmitter and receiver devices…Telecommunications devices include telephones, telegraph, radio, microwave communication arrangements, fiber optics, satellites and the Internet.'[975]

URL: An acronym for **U**niform **R**esource **L**ocator, a URL is the 'address that defines the route to a file on an Internet server (Web server, mail server, etc.). URLs are typed into a Web browser to access Web pages and files, and URLs are embedded within the pages themselves as links.'[976]

Web hosting: Making a Web site available on the Internet. A Web site contains pages of information stored in a Web server, which is a computer running Web server software connected to the Internet…Small [organizations] typically use a third party to host their site; however, sites with minimal traffic can share a single server with other low-traffic

---

973 'Social Media'. *Techopedia* Dictionary. http://www.techopedia.com/definition/4837/social-media (Accessed 25 October 2014.)
974 'Definition of: spider'. *PC Magazine* Encyclopedia. http://www.pcmag.com/encyclopedia/term/51860/spider (Accessed 24 October 2014.)
975 'Telecommunications'. *Techopedia* Dictionary. http://www.techopedia.com/definition/5570/telecommunications (Accessed 25 October 2014.)
976 'Definition of URL'. *PC World* Encyclopedia. http://www.pcmag.com/encyclopedia/term/53516/url (Accessed 25 October 2014.)

customers. In contrast, Web sites for large [organizations] may require dozens, hundreds or even thousands of Web servers.[977]

World Wide Web: 'An Internet-based system that enables an individual or a company to publish itself to the entire world, except to countries or locations that prohibit the free interchange of information.'[978]

977 'Definition of: Web hosting'. *PC World* Encyclopedia. http://www.pcmag.com/encyclopedia/term/54305/web-hosting (Accessed 25 October 2014.)

978 'Definition of; World Wide Web'. PC World Encyclopedia. http://www.pcmag.com/encyclopedia/term/54867/world-wide-web (Accessed 25 October 2014.)

Selected Bibliography

United Nations:

United Nations. 10 December 1948. The Universal Declaration of Human Rights. www.un.org/en/documents/udhr

Office of the United Nations High Commissioner for Human Rights. 23 March 1976. International Covenant on Civil and Political Rights. www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Office of the United Nations High Commissioner for Human Rights. 2011. Guiding Principles on Business and Human Rights. www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

United Nations Human Rights Council. 16 July 2012. The promotion, protection and enjoyment of human rights on the Internet. (A/HRC/RES/20/8). http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8

United Nations General Assembly. 20 November 2013. The right to privacy in the digital age. (UN Doc A/C.3/68/L.45/Rev.1. http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1

La Rue, Frank. 16 May 2011. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Office of the United Nations High Commissioner for Human Rights. (A/HRC/17/27). http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

La Rue, Frank. 10 August 2011. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (United Nations General Assembly document A/66/290). www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf

La Rue, Frank. 17 April 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Office of the United Nations High Commissioner for Human Rights. (A/HRC/23/40). www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Pillay, Navi. 30 June 2014. The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights. (A/HRC/27/37). www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

UNESCO

UNESCO. July 2014. Internet Universality: A Means towards Building Knowledge Societies and the Post-2015 Sustainable Development Agenda. Draft Proposed by the Secretariat. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/internet_universality_summary_240314_en.pdf

—. 2014. World Trends in Freedom of Expression and Media Development. Paris, UNESCO Publishing. www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/world-trends-in-freedom-of-expression-and-media-development

—. 2013. Draft Medium-Term Strategy: 2014–2021 (37 C/4). Paris, UNESCO Publishing. http://unesdoc.unesco.org/images/0022/002200/220031e.pdf

Dutton, William H., Anna Dopatka, Michael Hills, Ginette Law and Victoria Nash. 2011. Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet. Paris, UNESCO Publishing. http://unesdoc.unesco.org/images/0019/001915/191594e.pdf

Mendel, Toby, Andrew Puddephatt, Ben Wagner, Dixie Hawtin and Natalia Torres. 2012. Global Survey on Internet Privacy and Freedom of Expression. Paris, UNESCO Publishing. http://unesdoc.unesco.org/images/0021/002182/218273e.pdf

Other inter-governmental:

APEC Cross-Border Privacy Rules System http://www.cbprs.org/

Broadband Commission Working Group on Broadband and Gender. September 2013. Doubling Digital Opportunities: Enhancing the Inclusion of Women & Girls in the Information Society. Geneva, International Telecommunications Union. www.broadbandcommission.org/Documents/working-groups/bb-doubling-digital-2013.pdf

Council of Europe Committee of Ministers. 28 May 2003. Declaration on freedom of communication on the Internet. (Decl-28.05.2003E.) https://wcd.coe.int/ViewDoc.jsp?id=37031

Council of Europe. 16 April 2014. Recommendation of the Committee of Ministers to member States on a Guide to human rights for Internet users. (CM/Rec(2014)6.) https://wcd.coe.int/ViewDoc.jsp?id=2184807

European Commission. E-Commerce Directive. 4 May 2000. (2000/31/EC) http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm

European Commission. 28 November 2008. Framework Decision on Racism and Xenophobia. http://ec.europa.eu/justice/fundamental-rights/racism-xenophobia/framework-decision/index_en.htm

European Commission. 16 July 2013. Overview on Binding Corporate Rules. Data Protection. http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

European Parliament and the Council of the European Union. 22 May 2001. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. EUR-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001L0029

Edwards, Lilian. 22 June 2011. Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights. Geneva, World Intellectual Property Organisation. (WIPO-ISOC/GE/11/REF/01/EDWARDS). www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf

Ministers of the Freedom Online Coalition. Recommendations for Freedom Online. Adopted in Tallinn, Estonia on April 28, 2014 by https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf

Organization for Security and Co-operation in Europe. Decriminalization of defamation. www.osce.org/fom/106287

Organisation for Economic Co-operation and Development. September 2011. The Role of Internet Intermediaries in Advancing Public Policy Objectives. Paris, OECD Publishing. http://browse.oecdbookshop.org/oecd/pdfs/product/9311031e.pdf

Organisation for Economic Co-operation and Development. 13 December 2011. OECD Council Recommendation on Principles for Internet Policy Making. www.oecd.org/internet/ieconomy/49258588.pdf

Perset, Karine/OECD. March 2010. The Economic and Social Role of Internet Intermediaries. Paris, Organisation for Economic and Co-operation and Development, p. 9. (DSTI/ICCP(2009)9/FINAL.) www.oecd.org/internet/ieconomy/44949023.pdf

Other documents and resources

Access Now. Telco Remedy Plan https://www.accessnow.org/telco-remedy-plan

Broadband Stakeholder Group (UK). Voluntary industry code of practice on traffic management transparency for broadband services. http://www.broadbanduk.org/wp-content/uploads/2013/08/Voluntary-industry-code-of-practice-on-traffic-management-transparency-on-broadband-services-updated-version-May-2013.pdf

The Center for Internet and Society. July 2014. World Intermediary Liability Map (WILMap). Stanford, Calif., Stanford Law School. http://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap

Chilling Effects. http://www.chillingeffects.org

Global Network Initiative. Principles. http://www.globalnetworkinitiative.org/principles/

Global Network Initiative. Implementation Guidelines. https://globalnetworkinitiative.org/implementationguidelines/index.php

Necessary and Proportionate. 10 July 2013. International Principles on the Application of Human Rights to Communications Surveillance. https://en.necessaryandproportionate.org/text

Ofcom Report on Internet safety measures - Internet Service Providers: Network level filtering measures. Ofcom. 22 July 2014. http://stakeholders.ofcom.org.uk/internet/internet-safety-2?utm_source=updates&utm_medium=email&utm_campaign=filtering-report

Open Rights Group. Blocked! The personal cost of filters. July 2014. https://www.blocked.org.uk/personal-stories

Telecommunications Industry Dialogue on Freedom of Expression and Privacy. Guiding Principles. Version 1 6 March 2013. http://www.vodafone.com/content/dam/sustainability/pdfs/telecom_industry_dialogue_principles.pdf

Takedown Hall of Shame. Electronic Frontier Foundation. https://www.eff.org/takedowns

UC Berkeley Library. Invisible or Deep Web: What it is, How to find it, and Its inherent ambiguity. http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html

Who Has Your Back? 2014. Protecting Your Data From Government Requests. Electronic Frontier Foundation. https://www.eff.org/who-has-your-back-2014

Books, articles, and reports

African Gender Institute. December 2013. Feminist Africa, Vol. 18, 'e-spaces: e-politics'. http://agi.ac.za/sites/agi.ac.za/files/fa18_web-1.pdf

Alston, Philip (ed). 2005. *Non-State Actors and Human Rights*. Oxford, Oxford University Press.

Athique, Adrian. 2013. *Digital Media and Society: An Introduction*. Polity.

Bamman, David, Brendan O'Connor and Noah Smith. March 2012. Censorship and deletion practices in Chinese social media. First Monday, Vol. 17, No. 3. http://dx.doi.org/10.5210/fm.v17i3.3943

Bankston, Kevin, David Sohn and Andrew McDiarmid. December 2012. Shielding the Messengers: Protecting Platforms for Expression and Innovation. Washington DC, Center for Democracy and Technology. www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf

Bayley, Ed. 16 November 2009. The Clicks that Bind: Ways Users "Agree" to Online Terms of Service. Electronic Frontier Foundation. https://www.eff.org/wp/clicks-bind-ways-users-agree-online-terms-service

Bei Feng. 26 November 2012. Microblogs Have Become the Focus of Internet Censorship in China. Human Rights in China. www.hrichina.org/en/crf/article/6406

Benedek, Wolfgang and Matthias C. Kettemann. December 2013. Freedom of Expression and the Internet. Strasbourg, Council of Europe Publishing. https://book.coe.int/eur/en/human-rights-and-democracy/5810-freedom-of-expression-and-the-internet.html

Bently, Lionel and Brad Sherman. 2009. *Intellectual Property Law*, 3rd edn. Oxford, Oxford University Press.

Berger, Guy and Zikhona Masala. 22 March 2012. Mapping Digital Media: South Africa. New York, Open Society Foundations. www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-south-africa-20120416.pdf

Bergman, Michael K. August 2001. White Paper: The Deep Web: Surfacing Hidden Value. Taking License. Vol 7 Issue 1. http://quod.lib.umich.edu/j/jep/3336451.0007.104

Beschastna, Tatyana. 2014. Freedom of Expression in Russia as it Relates to Criticism of the Government. Emory International Law Review, Vol. 27, No. 2. http://law.emory.edu/eilr/content/volume-27/issue-2/comments/freedom-expression-russia.html

Black, Julia. January 1996. Constitutionalising Self-Regulation. The Modern Law Review, Vol. 59, No. 1, pp. 24–55. http://dx.doi.org/10.1111/j.1468-2230.1996.tb02064.x

BSR, with CDT. September 2014. Legitimate and Meaningful Stakeholder Engagement in Human Rights Due Diligence: Challenges and Solutions for ICT Companies. http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf

Budish, Ryan. 19 December 2013. What Transparency Reports Don't Tell Us. The Atlantic. www.theatlantic.com/technology/archive/2013/12/what-transparency-reports-dont-tell-us/282529

Business and Human Rights Resource Centre. September 2010. The UN 'Protect, Respect and Remedy' Framework for Business and Human Rights. www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-protect-respect-remedy-framework.pdf

Carter, Edward L. 2014. Argentina's Right to be Forgotten. Emory International Law Review, Vol. 27, No. 1. http://law.emory.edu/eilr/content/volume-27/issue-1/articles/argentinas-right-to-be-forgotten.html

Castells, Manuel. 2012. *Networks of Outrage and Hope: Social Movements in the Internet Age*. Cambridge, Polity.

Cheung, Anne S.Y. 2006. The Business of Governance: China's Legislation on Content Regulation in Cyberspace. New York University Journal of International Law and Politics. v. 38, p. 1-37 http://nyujilp.org/wp-content/uploads/2013/02/38.1_2-Cheung.pdf

Chin, Yik Chan. August 2013. Regulating social media. Regulating life (and lives). RJR 33 Online, http://journalism.hkbu.edu.hk/doc/Regulating_social-Media.pdf

China Internet Network Information Center (CNNIC). 2014 www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201401/P020140116395418429515.pdf

Christ, Roxanne E., Jeanne S. Berges and Shannon C. Trevino. July 2007. Social Networking Sites: To Monitor or Not to Monitor Users and Their Content? Intellectual Property and Technology Law Journal, Vol. 19, No. 7, pp. 1–6. www.lw.com/thoughtLeadership/social-networking-monitoring-content-texas-case

Comninos, Alex. October 2012. The Liability of Internet Intermediaries in Nigeria, Kenya, South Africa, and Uganda: An Uncertain Terrain. South Africa, Association for Progressive Communications. www.apc.org/en/system/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL.pdf

——. October 2012. Intermediary liability in South Africa. South Africa, Association for Progressive Communications. (Intermediary Liability in Africa Research Papers, No. 3). www.apc.org/en/system/files/Intermediary_Liability_in_South_Africa-Comninos_06.12.12.pdf

Cotter, Thomas F. 2005. Some Observations on the Law and Economics of Intermediaries. Michigan State Law Review, Vol. 1, pp. 1–16. (Washington & Lee Legal Studies Paper No. 2005-14). http://ssrn.com/abstract=822987

Dara, Rishabh. 2011. Intermediary Liability in India: Chilling Effects on Free Expression on the Internet. Bangalore, The Centre for Internet and Society. http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf

Das, Sauvik and Adam Kramer. 2013. Self-Censorship on Facebook. Proceedings of the Seventh International Association for the Advancement of Artificial Intelligence (AAAI) Conference on Weblogs and Social Media, pp. 120–27. www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350

Davies, Simon (ed). June 2014. A Crisis of Accountability: A global analysis of the impact of the Snowden revelations. Privacy Surgeon. www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf

Deibert, Ronald, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds). April 2010. Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. Cambridge, Mass., MIT Press. http://mitpress.mit.edu/books/access-controlled

DeNardis, Laura. August 2013. Internet Points of Control as Global Governance. Internet Governance Papers. No.2. Centre for International Governance Innovation. http://www.cigionline.org/sites/default/files/no2_3.pdf

Diamond, Larry. July 2010. Liberation technology. Journal of Democracy, Vol. 21, No. 3, pp. 69–83. www.journalofdemocracy.org/articles/gratis/Diamond-21-3.pdf

Epstein, Gady. 3 March 2011. Sina Weibo. Forbes Asia. www.forbes.com/global/2011/0314/features-charles-chao-twitter-fanfou-china-sina-weibo.html

Ghanea, Nazila. 2013. Intersectionality and the Spectrum of Racist Hate Speech: Proposals to the UN Committee on the Elimination of Racial Discrimination. Human Rights Quarterly, Vol. 35, No. 4, pp. 935–54. http://dx.doi.org/10.1353/hrq.2013.0053

Gillespie, Tarleton. 2010. The Politics of 'Platforms'. New Media & Society, Vol. 12, No. 3, pp. 347–64. http://dx.doi.org/10.1177/1461444809342738

Global Network Initiative. January 2014. Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo. http://globalnetworkinitiative.org/sites/default/files/GNI%20Assessments%20Public%20Report.pdf

Goodno, Naomi Harlin. 2007. Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws. Missouri Law Review, Vol. 72, No. 1, pp. 125–97, http://scholarship.law.missouri.edu/cgi/viewcontent.cgi?article=3985&context=mlr

Grabowicz PA, Ramasco JJ, Moro E, Pujol JM, Eguiluz VM. 2012. Social Features of Online Networks: The Strength of Intermediary Ties in Online Social Media. PLoS ONE, Vol. 7, No. 1. http://dx.doi.org/10.1371/journal.pone.0029358

Hannak, Aniko, Balachander Krishnamurthy, David Lazer, Christo Wilson, Arash Molavi Kakhki and Alan Mislove. Measuring Personalization of Web Search. WWW '13 Proceedings of the 22nd international conference on World Wide Web. pp. 527-538. http://www.ccs.neu.edu/home/cbw/pdf/fp039-hannak.pdf

Herpai, Gergely. Unsocial network: the rise and fall of iWiW. Budapest Business Journal. 7 January 2013. www.bbj.hu/business/unsocial-network-the-rise-and-fall-of-iwiw_64418

Hope, Dunstan Allison. February 2011. Protecting Human Rights in the Digital Age. BSR. https://globalnetworkinitiative.org/sites/default/files/files/BSR_ICT_Human_Rights_Report.pdf

Howard, Philip N. 2010. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford, Oxford University Press.

Hulin, Adeline (ed). 2013. Joint Declarations of the representatives of intergovernmental bodies to protect free media and expression. Vienna, Organization for Security and Co-operation in Europe. www.osce.org/fom/99558?download=true

Imre, Anikó. May 2009. National intimacy and post-socialist networking. *European Journal of Cultural Studies*, Vol. 12, No. 2, pp. 219–33.

The Institute for Human Rights and Business and Shift. June 2013. ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights. European Commission, www.shiftproject.org/publication/european-commission-ict-sector-guide

Intel Corporation and Dalberg Global Development Advisors. 2012. Women and the Web: Bridging the Internet Gap and Creating New Global Opportunities in Low and Middle-Income Countries. www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf

Internet Watch Foundation. 2013. Internet Watch Foundation Annual & Charity Report 2013. Cambridge, IWF, p. 5. www.iwf.org.uk/assets/media/annual-reports/annual_report_2013.pdf.pdf

Internet Users by Country. 2014. Internet Live Stats. www.internetlivestats.com/internet-users-by-country

Jellema, Anne and Karin Alexander. 22 November 2013. 2013 Web Index Report. Geneva, World Wide Web Foundation. http://thewebindex.org/wp-content/uploads/2013/11/Web-Index-Annual-Report-2013-FINAL.pdf

Jiang, Min. The Business and Politics of Search Engines: A Comparative Study of Baidu and Google's Search Results of Internet Events in China. New Media & Society. 16(2). http://www.researchgate.net/publication/256016569_The_Business_and_Politics_of_Search_Engines_A_Comparative_Study_of_Baidu_and_Googles_Search_Results_of_Internet_Events_in_China.

Johnson, Eric J., Steven Bellman and Gerald L. Lohse. 2002. Defaults, Framing, and Privacy: Why Opting In–Opting Out. *Marketing Letters*, Vol. 13, No. 1.

Kalemera, Ashnah. 20 June 2014. Uganda: When National Security Trumps Citizens' Internet Freedoms. OpenNet Africa. http://opennetafrica.org/internet-freedom-in-uganda-personal-information-and-the-state

——, Lillian Nalwoga and Wairagala Wakabi. Intermediary Liability in Uganda. CIPESA. www.apc.org/en/system/files/Intermediary_Liability_in_Uganda.pdf

Kamdar, Adi. 6 December 2012. EFF's Guide to CDA 230: The Most Important Law Protecting Online Speech. EFF Deeplinks Blog. https://www.eff.org/deeplinks/2012/12/effs-guide-cda-230-most-important-law-protecting-online-speech

KVG Research. December 2013. TV Market and Video on Demand in the Russian Federation. Strasbourg, European Audiovisual Observatory. www.obs.coe.int/documents/205595/552774/RU+TV+and+VoD+2013+KVG+Research+EN.pdf/5fbb076c-868e-423a-bfed-dca8b66cac43

Lengyel, Balázs, Attila Varga, Bence Ságvári and Ákos Jakobi. 26 January 2013. Distance dead or alive Online Social Networks from a geography perspective. SSRN. http://dx.doi.org/10.2139/ssrn.2207352

Marthews, Alex and Catherine Tucker. 24 March 2014. Government Surveillance and Search Behavior. SSRN. http://ssrn.com/abstract=2412564.

MacKinnon, Rebecca. 2 February 2009. China Censorship 2.0: How Companies Censor Bloggers. First Monday, Vol. 14, No. 2. http://firstmonday.org/article/view/2378/2089

——. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York, Basic Books.

Maireder, Axel and Stephan Schlögl. 17 February 2014. 24 Hours of an #outcry: The Networked Publics of a Socio-Political Debate. European Journal of Communication, Vol. 29, forthcoming, http://homepage.univie.ac.at/axel.maireder/php/wordpress/wp-content/MairederSchloegl_24HoursOfAnOutcry_PrePrint.pdf

Marsden, Christopher T. 2011. *Internet Co-Regulation: European Law, Regulatory Governance, and Legitimacy in Cyberspace*. Cambridge, Cambridge University Press.

McNamee, Joe. January 2011. The Slide from Self-Regulation to Corporate Censorship. Brussels, European Digital Rights Initiative. www.edri.org/files/EDRI_selfreg_final_20110124.pdf

Munyua, Alice. Kenya: Perceptions and Misconceptions: The Role of New and Traditional Media in Kenya's Post Election Violence. GIS Watch and Kenya ICT Action Network (KICTANet). 2011. http://www.giswatch.org/sites/default/files/gisw_-_kenya.pdf

Munyua, Alice, Grace Githaiga and Victor Kapiyo. 2012. Intermediary Liability in Kenya. Kenya ICT Action Network, www.apc.org/en/system/files/Intermediary_Liability_in_Kenya.pdf

Natour, Faris and Pluess, Jessica Davis. March 2013. Conducting an Effective Human Rights Impact Assessment. BSR. http://www.bsr.org/reports/BSR_Human_Rights_Impact_Assessments.pdf

Nash, Victoria. 2013: Analyzing Freedom of Expression Online: Theoretical, empirical, and normative contributions, in: Dutton, W.H. (eds.) The Oxford Handbook of Internet Studies, Oxford University Press.

Nyst, Carly. End violence: Women's rights and safety online project – Internet intermediaries and violence against women online. Executive summary and findings'. Association for Progressive Communications (APC). July 2014. http://www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf

OpenNet Initiative. About Filtering. https://opennet.net/about-filtering

Palfrey, John G. Jr. Local Nets on a Global Network: Filtering and the Internet Governance Problem. The Global Flow of Information. Jack Balkin, ed. Harvard Public Law Working Paper No. 10-41. p.8. Available at SSRN: http://ssrn.com/abstract=1655006.

Parti, Katalin and Luisa Marin. 2013. Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A Comparative Analysis on Blocking Measures and Internet Providers' Removal of Illegal Internet Content. Journal of Contemporary European Research, Vol. 9, No. 1, pp. 138–59. www.jcer.net/index.php/jcer/article/view/455/392

Pasquale, Frank A. 2010. Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries. Northwestern University Law Review, Vol. 104, No. 1, pp. 105–74. www.law.northwestern.edu/lawreview/v104/n1/105/LR104n1Pasquale.pdf

PEN American Center. 12 November 2013. Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor. PEN American Center. www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

Purdon, Lucy. November 2013. Corporate Responses to Hate Speech in the 2013 Kenyan Presidential Elections. Case Study: Safaricom. Institute for Human Rights and Business. (Digital Dangers: Identifying and Mitigating Threats in the Digital Realm.) www.ihrb.org/pdf/DD-Safaricom-Case-Study.pdf

Qian Tao. 2011. Intermediary Liability of Website Operators in Privacy Cases in China. Masaryk University Journal of Law and Technology, Vol. 5, No. 1, pp. 105–18. http://mujlt.law.muni.cz/storage/1327951355_sb_09-tao.pdf

Ramzy, Austin. 17 February 2011. Wired Up. Time. http://content.time.com/time/printout/0,8816,2048171,00.html

Rosenberg, R. S. 2011. Controlling access to the Internet: The role of filtering. Ethics and Information Technology, Vol. 3, No. 1, pp. 35–54. www.copacommission.org/papers/rosenberg.pdf

Rotenberg, Marc and David Jacobs. 2013. Updating the Law of Information Privacy: The New Framework of the European Union. Harvard Journal of Law & Public Policy, Vol. 36, No. 2, pp. 605–52. www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_605_Rotenberg_Jacobs.pdf

Rustad, Michael L. and D'Angelo, Diane. 2012. The Path of Internet Law: An Annotated Guide to Legal Landmarks. Duke Law & Technology Review. Vol. 2011, No. 012. Suffolk University Law School Research Paper No. 11-18. Available at SSRN: http://ssrn.com/abstract=1799578

Samway, Michael A. Business, Human Rights and the Internet: A Framework for Implementation. in *Human Dignity and the Future of Global Institutions.* (eds. Arend and Lagon, Georgetown University Press, 2014)

Savin, Andrej and Jan Trzaskowski, eds. *Research Handbook on EU Internet Law*. (Edward Elgar Publishing, 2014).

Sceats, Sonya and Shaun Breslin. October 2012. China and the International Human Rights System. London, Chatham House. www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/r1012_sceatsbreslin.pdf

Seltzer, Wendy. Fall 2010. Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment. Harvard Journal of Law & Technology, Vol. 24, No. 1, pp. 171–232. http://jolt.law.harvard.edu/articles/pdf/v24/24HarvJLTech171.pdf

Seng, Daniel and Ignacio Garrote Fernandez-Diez. 2012. Comparative Analysis of National Approaches of the Liability of the Internet Intermediaries. Geneva, World Intellectual Property Organization. www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf

Sieminski, Paul. 21 November 2013. Striking Back Against Censorship. WordPress Hot Off the Press Blog. http://en.blog.wordpress.com/2013/11/21/striking-back-against-censorship

Simon, Joel (ed). 6 May 2014. Halftime for the Brazilian press: Will justice prevail over censorship and violence? New York, Committee to Protect Journalists. https://cpj.org/reports/brazil2014-english.pdf

Soldatov, Andrei and Irina Borogan. 4 March 2013. Lawful interception: the Russian approach. https://www.privacyinternational.org/blog/lawful-interception-the-russian-approach

Sparas, Denis. 18 June 2013. EU regulatory framework for e-commerce. World Trade Organization Workshop on E-Commerce. Geneva, World Trade Organization. www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/sparas_e.pdf

Sunstein, Cass. December 2013. Deciding by Default. University of Pennsylvania Law Review, Vol. 162, No. 1. http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1000&context=penn_law_review

Tóth, Borbála. 5 January 2012. Mapping Digital Media: Hungary. Open Society Foundations. p. 42. www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-hungary-20120216.pdf

Tuppen, Chris. 2012. Opening the Lines: A Call for Transparency from Governments and Telecommunications Companies. Global Network Initiative. https://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf

Van Hoboken, Joris. Search Engine Freedom: On the implications of the right to freedom of expression for the legal governance of Web search engines. PhD thesis, University of Amsterdam Faculty of Law, 2012. http://dare.uva.nl/document/357527

Villeneuve, Nart. January 2006. The Filtering Matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace. First Monday. Vol. 11. No. 1-2.

Xu, Xueyang, Z. Morley Mao, and J. Alex Halderman. Internet Censorship in China: Where Does the Filtering Occur? In Proceedings of PAM . 2011. http://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf

Yan Mei Ning. Summer 2011. Criminal Defamation in the New Media Environment – The Case of the People's Republic of China. International Journal of Communications Law & Policy, Vol. 14, pp. 1–91. http://ijclp.net/ojs/index.php/ijclp/article/view/15/5

York, Jillian C. September 2010. Policing Content in the Quasi Public Sphere. OpenNet Initiative. https://opennet.net/policing-content-quasi-public-sphere

Yu, Allen. 23 March 2012. Carnegie Mellon Study on Censorship and Deletion Practices in Chinese Social Media. Stanford Law School Center for Internet and Society Blog. http://cyberlaw.stanford.edu/blog/2012/03/carnegie-mellon-study-censorship-and-deletion-practices-chinese-social-media

Zingales, Nicolo. November 2013. Internet intermediary liability: Identifying best practices for Africa. South Africa, Association for Progressive Communications. www.apc.org/en/system/files/APCInternetIntermediaryLiability_BestPracticesAfrica_20131125.pdf

Zittrain, Jonathan and John Palfrey. 2008. Internet Filtering: The Politics and Mechanisms of Control. In Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds. *Access Denied: The Practice and Policy of Global Internet Filtering.* (Cambridge: MIT Press)

——. Spring 2006. A History of Online Gatekeeping. Harvard Journal of Law & Technology, Vol. 19, No. 2, pp. 253–98. http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf

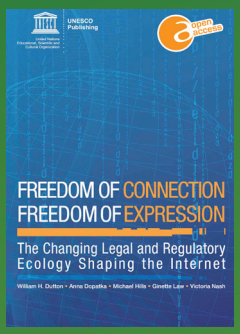
Zuckerman, Ethan. April 2010. Intermediary Censorship. Ronald Deibert (ed.), Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. Cambridge, Mass., MIT Press, pp. 71–85. www.access-controlled.net/wp-content/PDFs/chapter-5.pdf

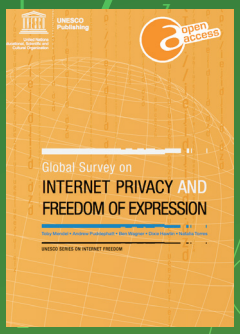
"UNESCO, as enshrined in its Constitution, promotes the "free flow of ideas by word and image", and is accordingly committed to enabling a free, open and accessible Internet space as part of promoting comprehensive freedom of expression online and offline.

We believe the rich material in this, the third in UNESCO Series on Internet Freedom, will be of great value to all stakeholders. These are industry actors, UNESCO Member States, technical community, Intergovernmental organizations, private sector, civil society, and others both national and international."

Getachew Engida
Deputy Director-General of UNESCO

UNESCO SERIES ON INTERNET FREEDOM





UNESCO thanks the Open Society Foundations, the Internet Society, and the Center for Global Communication Studies at the University of Pennsylvania's Annenberg School for Communication for their financial and administrative support to the research.

United Nations
Educational, Scientific and
Cultural Organization

Communication and
Information Sector

9 789231 000393