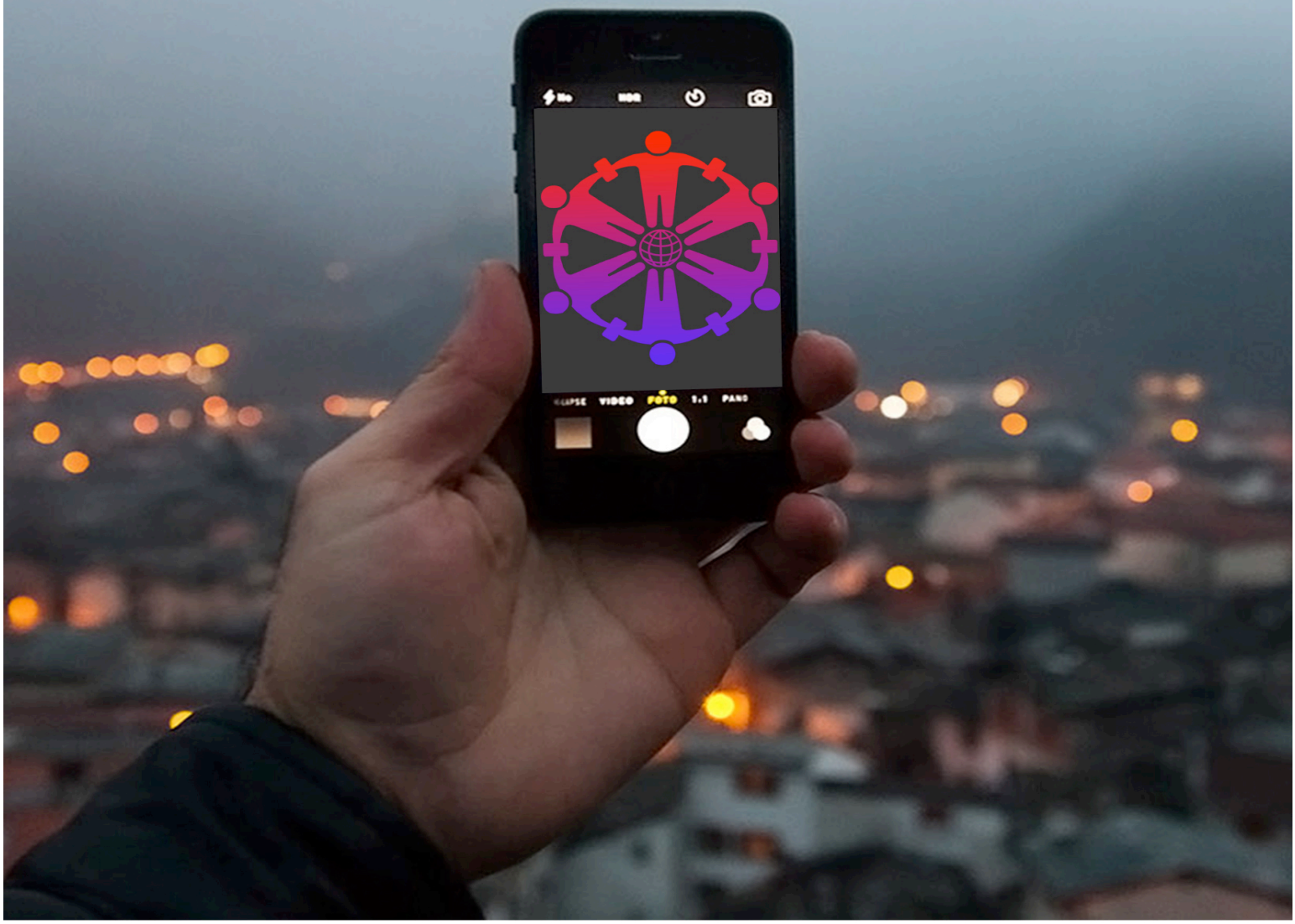
CENTRE FOR LAW AND DEMOCRACY

Stand Up for Digital Rights

Recommendations for Responsible Tech



THE CENTRE FOR INTERNET & SOCIETY

CIPPIC

OPENNET

Arabic Network for Human Rights Information

CELE

Stand Up for Digital Rights!

Recommendations for Responsible Tech

Centre for Law and Democracy (CLD)

39 Chartwell Lane
Halifax, N.S.
B3M 3S7
Canada

Tel: +1 902 431-3688
Fax: +1 902 431-3689
Email: info@law-democracy.org
www.law-democracy.org
Twitter: @Law-Democracy

Acknowledgements

This publication was drafted by Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy, with editing and support from Toby Mendel, Executive Director, Centre for Law and Democracy. Additional material was provided by the Arabic Network for Human Rights Information, the Centre for Internet and Society, the Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Open Net Korea, Tamir Israel and Christopher Parsons. Additional research was provided by CLD's interns and pro bono students: Pierre-Luc Bergeron, Alice Bodet-Lamarche, Jim Boyle, Ken Cadigan, Paul Calderhead, Laurent Fastrez, Claire MacLean, Jonathan Marchand, Charles McGonigal, Virginia Nelder and Leslie Whittaker.

It was also produced with the assistance of an Advisory Panel of leading digital rights experts: Farieha Aziz, BoloBhi; Anriette Esterhuysen, Association for Progressive Communications; Ahmad Faisol, Media Link; Grace Githaiga, Kenya ICT Action Network, KICTAnet; Ang Peng Hwa, Wee Kim Wee School of Communication and Information, Asian Media Information and Communication Centre; David Kaye, UC Irvine School of Law, UN Special Rapporteur on the Right to Freedom of Opinion and Expression; Emma Llansó, Director of the Free Expression Project, Center for Democracy and Technology; Raegan MacDonald, Senior EU Policy Manager, Mozilla; Rebecca MacKinnon, Director, Ranking Digital Rights; Peter Nestor, Manager, Advisory Services, Human Rights, Business for Social Responsibility; Danny O'Brian, Electronic Frontiers Foundation; Andy O'Connell, Manager, Global Policy Development, Facebook; Patrick Robinson, Head of Public Policy, EMEA & Canada, Airbnb; Claudio Ruiz. Executive Director, Derechos Digitales; Alex Walden, Google; Cynthia Wong, Human Rights Watch.

The production of this report was made possible thanks to support from the International Development Research Centre (IDRC). This support does not necessarily imply that the IDRC endorses the positions taken in this report, and the Centre for Law and Democracy is responsible for the presentation of the facts and opinions contained in this report.

Executive Summary

Recent years have seen the formation of private sector empires in the online world that hold unprecedented power over how people access information and communicate. Although these tech giants earned their position by developing new and innovative products, and their businesses support the spread of the Internet, the growing power of private sector intermediaries[1] over online communications has important implications. The enormous impact their policies and practices have on the exercise of key rights means that they are on the cutting edge of the application of new ideas about the human rights responsibilities of private actors.

An important starting point for any discussion about human rights and the Internet is that human rights standards apply to the online world. The Internet supports the promotion and protection of a number of human rights, most obviously freedom of expression but also the rights to association, to education, to work, to participate and to take part in cultural life, among others. The UN Human Rights Council[2] and the UN General Assembly[3] have both affirmed that human rights standards apply to the online world. The Internet supports human rights by improving communications and information sharing, by providing a voice for human rights defenders, and by strengthening democratic society through its contribution to political, social, cultural and economic development. However, the role that private sector intermediaries play in providing access to, managing, facilitating and mediating online speech presents a key challenge to guaranteeing human rights on the Internet, particularly as traditionally public avenues for expression, such as the postal service, are being replaced by private services.

Although States bear the primary obligation for ensuring respect for human rights, it is now recognised that private sector actors also have a direct responsibility to respect and to foster respect for human rights. A key issue for guaranteeing freedom of expression on the Internet is the role that online intermediaries play in providing access to, managing, facilitating and mediating online speech. Rather than creating a platform for an influential few, as newspapers or broadcasters do, Internet intermediaries facilitate speech directly by individuals, giving everyone a platform and access to a global audience. By the same token, however, this grants these intermediaries an unprecedented influence over individuals' right to freedom of expression and access to information. This power has also attracted the attention of State actors, which are placing increasing pressure on online intermediaries to

[1] We define "intermediaries" as private sector bodies whose online operations somehow, whether directly or indirectly, facilitate communication between two or more parties over the Internet.
[2] Resolution A/HRC/20/L.13, 29 June 2012. Available at: www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc.
[3] Resolution A/C.3/68/L.45/Rev.1, 26 November 2013. Available at: www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1.

facilitate and/or participate in human rights violations, for example by supporting intrusive surveillance systems or acting to police user content.

In recent years, there has been an increasing focus on the human rights implications of the policies and practices of intermediaries. The most high profile work on human rights and the private sector in general is the 2011 *Guiding Principles on Business and Human Rights*,[4] which was developed under the auspices of the United Nations. However, recent years have seen the launch of programmes aimed specifically at the tech sector, such as the Global Network Initiative[5] and the Ranking Digital Rights Project.[6]

There are three layered challenges which any initiative to promote good practice in the private sector faces. The first is engagement in the sense of simply getting major private sector actors to the table. The second is transparency, in terms of being able to access corporate information in order to assess performance, and then of being able to publish the results of those assessments. The third is actually fostering change, and convincing companies to amend policies or practices which are problematic or which do not represent better practice.

These are significant challenges, which are in some respects more complicated than efforts to promote human rights at the State level (itself no easy task). Furthermore, solidarity from States in promoting respect by other States is common, whether conducted on a bilateral basis or through intergovernmental organisations, while the presence of strong competition tends to undermine such solidarity among private companies. Nonetheless, the growing importance of intermediaries in this area means that the human rights community must face these challenges, and work to promote greater respect for human rights by intermediaries. The major areas of engagement can be divided thematically into six key issues, as spelled out in the following sections.

Expanding Access

Expanding access to the Internet is key to promoting human rights on the Internet, so that the benefits conferred may be enjoyed as widely as possible. Over the past decades, significant access gaps have emerged, including between developed and developing countries, between urban and rural populations and, most importantly,

[4] UN OHCHR, Guiding Principles On Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, 16 June 2011, HR/PUB/11/04. Available at: www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.
[5] See: www.globalnetworkinitiative.org.
[6] Rebecca Mackinnon, "The Ranking Digital Rights 2015 Corporate Accountability Index is now online!", Ranking Digital Rights, 3 November 2015. Available at: rankingdigitalrights.org/.

between the better off and the poor.[7] These discrepancies are the result of various factors. For example, urban areas are smaller and have a higher population density, and are thus easier and cheaper to connect. Cost differentials may be passed on to consumers, even though urban dwellers tend to be wealthier than rural ones. Intermediaries, and particularly access providers, can play a role in helping to overcome these divides by taking action to mitigate or eliminate pricing differentials between rural and urban customers. Access providers should also work directly to expand access, by investing a reasonable proportion of their profits in creating new infrastructure, including potentially through entering into public-private partnerships to this end.

While costs and a lack of infrastructure are major challenges to expanding access, linguistic or social barriers also inhibit the Internet's spread. These challenges can be self-reinforcing, since the lack of a likeminded community online can lead to a dearth of relevant content, further reducing the interest of members of that group in connecting. Again, intermediaries have an important role to play in overcoming these barriers, for example by promoting the development of content of relevance to less connected communities or in smaller languages.

Beyond their responsibility to help expand access, it is important to consider the role intermediaries can play vis-à-vis State efforts to limit access, for example by cutting off or denying service to users. These measures are highly intrusive and almost never justified according to international standards regarding freedom of expression. Where a government demands that an access provider cut off or deny service to a user or group, the provider should consider the broader human rights implications and any viable alternatives. Providers should also resist these demands to the extent that this is reasonable and should, as far as this is legally permitted, be transparent about requests they receive to cut off access.

Net Neutrality

As the Internet has grown, and become more lucrative, the ongoing debate about the foundational principle of network neutrality has sharpened. The core idea behind this principle is that intermediaries should not favour or disfavour (discriminate against) the transmission of certain types of Internet traffic.[8] There are several reasons why net neutrality is fundamentally important, including that it promotes free competition and that it limits the ability of private intermediaries to control online speech and debates.

---

[7] Brahima Sanou, ICT Facts & Figures (May 2015: International Telecommunication Union (ITU) Telecommunication Development Bureau). Available at: www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

[8] There are recognised exceptions to this rule, such as where necessary to protect the integrity or security of a network or to combat spam. For a more detailed description of these issues, see: www.thisisnetneutrality.org/.

States have approached this issue in different ways. Although the Internet and the way it is used are constantly changing, and there is no single and immutable rule for how networks should be managed, certain fundamental principles should guide intermediaries in this area. First and foremost, policies and technical protocols for managing Internet traffic should aim to improve the functioning of the Internet for all users, rather than favouring traffic from or to users who pay a premium or who have preferential or partnership arrangements. Transparency is also important, including publishing information about policies and technical protocols for managing traffic and periodic reports providing summaries about how traffic and information was handled. Where net neutrality principles are codified in law, intermediaries should respect this and avoid lobbying for change. Where the law is unclear or unsettled, they should still act in ways that respect the core principles of network neutrality.

A particularly contentious aspect of the net neutrality debate concerns zero rating schemes, which provide cheap or free access to the Internet but only give access to a limited range of services. Free Basics, a Facebook-led initiative which essentially provides people with free access to a few Internet services, including Facebook, is among the most well known zero rating schemes. Its proponents claim that by offering users a stripped-down version of the Internet for free, Free Basics generates interest in the Internet among new potential users, who can then move on to pay for a full connection. However, Free Basics has also faced criticism for failing to respect the principle of net neutrality and has even been banned by some regulatory agencies.[9] Although it can be argued that the harm inherent in zero rating schemes is outweighed by their benefit in bringing new people online, other schemes for providing an "on ramp" to the Internet do not compromise net neutrality. As a result, and due to the broad public interest in protecting net neutrality, the onus rests on intermediaries which have proposed or are operating zero rating schemes which compromise net neutrality to demonstrate that they are clearly more effective in terms of bringing people online than schemes which respect net neutrality and that the benefits are significant enough to justify these compromises.

Moderation and Removal of Content

Among the major factors behind the success of the Internet has been the open, honest and freewheeling nature of online discourse. By the same token, the sense of anonymity that is associated with being behind a computer or mobile screen can also encourage people's darker impulses and the Internet is a prime vehicle for vitriol and threats, as well as for the distribution of illegal material. This places intermediaries in a difficult position. On the one hand, for many the free flow of information is their bread and butter. On the other hand, their growing influence

[9] The most energetic campaign against Free Basics has emerged in India under the banner "Save the Internet". A summary of arguments against the programme is available at: blog.savetheinternet.in/what-facebook-wont-tell-you-about-freebasics/.

has placed them under increasing pressure, including from their own users, to mitigate the less desirable forms of online speech. Gender-based harassment is notoriously endemic online, although it is only part of a broader "civility" problem.

This has led some intermediaries to engage in more active content management which, in turn, has given rise to difficult challenges in determining when and how forcefully to intervene. It is conceptually easy to defend a laissez-faire approach, where companies only intervene when they are legally required to do so, on freedom of expression grounds. Once companies choose to go beyond that, the debate becomes far more tangled. In 2014, Twitter reacted energetically against the spread of propaganda messages about the murder of journalist James Foley at the hands of the Islamic State.[10] Although few would fault them for taking this stand, it inevitably led to questions as to why they had not been similarly proactive in working to combat sexual or racial harassment.[11] In 2012, a series of articles drew attention to forums on Reddit devoted to sexualising underage girls. Reddit ultimately decided to ban the content, a decision their users contrasted with the website's continued hosting of a forum devoted to pictures of dead children.[12]

Ultimately, private sector intermediaries have considerable flexibility in terms of the material they classify as offensive or against the standards of their services, but clear communication and strong procedural protections are essential. Content moderation should be based on clear, pre-determined policies which can be justified by reference to a standard based on objective criteria (such as providing a family friendly service) and which are described clearly in the policy. Ideally, intermediaries should consult with their users when determining such policies. In addition, intermediaries should post clear, thorough and easy to understand guides to their policies and practices, carefully scrutinising complaints and applying their policies consistently.

Beyond intermediaries' self-imposed standards, significant issues arise in the context of how they respond to illegal material. A major factor here is whether, and under what circumstances, intermediaries are themselves protected against liability for content in relation to which they provide services. Many legal systems condition immunity on intermediaries removing problematic content once they have been notified about it. Experience suggests that this approach is ripe for abuse, particularly in the case of copyright. Frivolous copyright removal requests are frequently used as a tool to quash political dissent or remove information that a

[10] Shane Harris, "Social Media Companies Scramble to Block Terrorist Video of Journalist's Murder", Foreign Policy, 19 August 2014. Available at: foreignpolicy.com/2014/08/20/social-media-companies-scramble-to-block-terrorist-video-of-journalists-murder/.
[11] James Ball, "Twitter: from free speech champion to selective censor?" The Guardian, 21 August 2014. Available at: www.theguardian.com/technology/2014/aug/21/twitter-free-speech-champion-selective-censor?CMP=twt_gu.
[12] "Why is it that r/jailbait was shut down, but not r/picsofdeadkids?", Reddit, 7 September 2012. Available at: www.reddit.com/r/AskReddit/comments/zhd5d/why_is_it_that_rjailbait_was_shut_down_but_not/.

person or organisation finds embarrassing or inconvenient. Automated systems to flag copyrighted material have been found to make mistakes and they are generally unable to take into account possible defences to copyright infringement, such as fair practice (known as fair use or fair dealing in some jurisdictions).

Intermediaries obviously wish to shield themselves against legal liability. However, many also go significantly beyond minimum legal requirements. In order to combat misuse, it is important to build strong procedural protections into systems for addressing illegal content. Users whose content is subject to removal should, whenever this is legally permissible, be notified promptly and provided with information about the process and any opportunities to mount a defence. Intermediaries should also try to devise solutions which are minimally intrusive and as targeted as possible. Where an intermediary determines that content should be removed, they should retain the means to reverse that action for as long as any appeal against the decision is pending, and should offer users the option to preserve and export their data, unless it is patently illegal.

Addressing Privacy Concerns Online

The right to privacy is recognised internationally as a human right, guaranteed in the *International Covenant on Civil and Political Rights*[13] and in most national constitutions. Privacy is also closely correlated with freedom of expression. Studies have shown that perceptions of control over one's communications, including over who has access to them, lead to franker and more extensive communications, while a loss of control leaves people feeling less free to engage earnestly.[14]

The Internet has had a dramatic impact on our understandings of the very concept of privacy. On the one hand, the Internet provides for an unprecedented level of freedom and anonymity. For a gay Ugandan or Russian, or a Saudi atheist, the Internet may provide the only avenue for self-expression or to network with likeminded communities. On the other hand, the Internet is also the most heavily monitored and tracked medium of expression in history, where every move that users make is noted, followed and recorded.

The collection and sale of personal information represents a core business model for many intermediaries. There are benefits to this, primarily in the form of allowing users to access services free of direct charges. But, even if one embraces the idea of exchanging privacy for free services online, States have a responsibility to protect

[13] UN General Assembly Resolution 2200A(XXI), 16 December 1966, in force 23 March 1976.
[14] Tamara Dinev, Heng Xu, Jeff H. Smith and Paul Hart, "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts" 22 European Journal of Information Systems (2013), p. 300. Available at: www.palgrave-journals.com/ejis/journal/v22/n3/pdf/ejis201223a.pdf.

consumers in these relationships.[15] It is arguable that the intrusiveness of State regulation over companies in this area should depend, at least in part, on the extent to which industry acts to offer effective protections of its own.

A key issue here is being clear and transparent with users about policies regarding the collection, sharing and processing of information. For example, users may implicitly understand that their private information is being processed by companies whose business model is based on advertising, but may not expect the same treatment from companies which impose up-front charges for their services.[16] Similarly, users may think that information will be tracked only in an automated or aggregated way, and assume that it will not be examined by human beings.[17] There is a particular need for clarity around the involvement of third party data brokers, who generally have no direct relationship with the users and who often collate information from multiple sources, which can significantly compound the privacy interference.[18]

Although all companies have a duty to respect user privacy, those which explicitly market the privacy features of their services have a particular obligation to avoid privacy intrusive behaviour.[19] Intermediaries should not let their commercial interests undermine their obligation to make realistic representations to users about privacy and to respect these commitments.

Anonymous communication is a particularly important area of debate regarding online privacy. At a cultural level, many online communities have strong taboos against doxxing or publishing personally identifiable information about a person using an online alias.[20] Anonymity is particularly important in terms of facilitating communication about sensitive subjects, such as sexual or mental health issues or child abuse, and enabling whistleblowing. Websites like Wikileaks could not exist without the promises of anonymity which they provide. The central role the Internet

---

[15] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, para. 58. Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. See also Human Rights Committee, General Comment 16, 8 April 1988. Available at: tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en.

[16] Andy Greenberg, "How to Stop Apple From Snooping on Your OS X Yosemite Searches", Wired, 20 October 2014. Available at: www.wired.com/2014/10/how-to-fix-os-x-yosemite-search/.

[17] Andrew Crocker, "Microsoft Says: Come Back with a Warrant, Unless You're Microsoft", Electronic Frontier Foundation, 21 March 2014. Available at: www.eff.org/deeplinks/2014/03/microsoft-says-come-back-warrant-unless-youre-microsoft.

[18] Timothy Libert, "Exposing the Hidden Web: Third-Party HTTP Requests on One Million Websites, International Journal of Communication, October 2015. Available at: ijoc.org/index.php/ijoc/article/download/3646/1503.

[19] See, for example, Paul Lewis and Dominic Rushe, "Revealed: how Whisper app tracks 'anonymous' users", The Guardian, 16 October 2014. Available at: www.theguardian.com/world/2014/oct/16/-sp-revealed-whisper-app-tracking-users.

[20] See: "What doxxing is, and why it matters", The Economist, 10 March 2014. Available at: www.economist.com/blogs/economist-explains/2014/03/economist-explains-9.

plays in disseminating sensitive communications means that failures on this front can have especially severe consequences.

This is not to suggest that all intermediaries have a responsibility to allow people to use their services anonymously. Some intermediaries have legitimate reasons for requiring real-name registration. However, decisions about this should take into account the broader human rights implications and the impact that the requirement may have on users. In particular, intermediaries should not require real-name registration where it would significantly harm the rights of their users. Perceptions, and building realistic expectations, are of cardinal importance here, and intermediaries have a responsibility to be transparent with their users as to the extent to which any anonymity they offer or appear to be offering will be respected.

Another key user privacy issue is data security, including the use of encryption.[21] An increasing number of intermediaries are encrypting more user information by default.[22] This is a welcome shift, and intermediaries should also consider taking action to encourage stronger security practices among their users, for example by offering inducements for good practice. Beyond storing information in encrypted formats whenever this is operationally and legally possible and supporting end-to-end encryption for users, data minimisation is another important factor in limiting privacy risks.[23] Once security has been breached, it is essential that intermediaries inform those who might have been impacted promptly and fully, since speed can be of the essence in mitigating the harm.

A final privacy issue is the right to be forgotten. In 2014, the European Court of Justice (ECJ) held that EU citizens had a right to request that search engines not display results relating to them which were "inadequate, irrelevant, or no longer relevant, or excessive in relation to the purposes for which they were processed".[24] There are legitimate concerns regarding how the Internet preserves and presents information about peoples' pasts. At the same time, there are significant problems with this judgment, particularly its failure to consider sufficiently the freedom of expression interests at play.

The decision is also problematic insofar as it places responsibility for implementation on search engines. Decisions about removing content should ideally be made by expert, public decision-makers, not private search engines. However,

---

[21] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 22 May 2015, para. 56-63.
[22] Lorenzo Franceschi-Bicchierai, "Reddit Switches to Encryption By Default", Motherboard, 17 June 2015. Available at: motherboard.vice.com/read/reddit-switches-to-https-encryption-by-default.
[23] Federal Trade Commission, *Internet of things: Privacy and Security in a Connected World*, January 2015. Available at: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[24] Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:2014:317. Available at: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

having been given this responsibility, search engines should implement it as fairly and transparently as possible. This should include consulting with key stakeholders to develop detailed policies and standards regarding how they enforce the right to be forgotten. Search engines should also, as far as possible, respect due process rights when applying the right to be forgotten, including by informing those whose content is subject to a removal request, as far as this is legally permitted, and by giving them an opportunity to argue that the material should not be blocked, including because the public interest lies in continuing to display the content.

Transparency and Informed Consent

The Internet has fundamentally changed our relationship with information, which has led to demand for greater openness on the part of intermediaries. This is particularly true in terms of users' personal information, where there is a broadly recognised right to track how it is being stored and processed.[25] The publication of certain types of information is also vital to facilitate informed consumer choices, including to allow people to choose companies whose policies align with their priorities and values.

An important openness tool is transparency reporting, which has become relatively common among major tech firms. Although the specific information provided varies, the central aims are generally to profile requests to take down content and government attempts to access user information. Better practice is to provide as much detail as possible here, including by subdividing statistics according to the underlying basis for the request, the type and location of the requester, the date of the request, how the user who was the subject of the complaint was notified and after what period of time, and how the request was disposed of. Information about the nature and processing of requests by governments for user information should be made available as far as such disclosures are legally permitted. Intermediaries should also publish information about their own enforcement of their terms of service, including where content is automatically flagged by a particular algorithm or where users have their accounts deleted for committing some sort of prohibited action.

Ideally, transparency reporting should be standardised across particular categories of intermediaries, although there are significant practical and legal complications to achieving this. At present, the differences in reporting make it difficult to compare policies and practices among actors operating in the same industry sector.

Beyond transparency reporting, published terms of service are an important vehicle for openness. Unfortunately, users seldom engage with these documents, despite the fact that they serve as the legal basis for the relationship between the company and

[25] Human Rights Committee, General Comment 16, 8 April 1988. Available at: tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en.

its users. In many cases, this includes the core agreement whereby users trade their privacy for services, an exchange which is predicated on informed consent. The fact that users so rarely pay attention to the content of terms of service also gives companies a licence to draft these terms broadly and/or in a deliberately obscure manner. For many companies, it is difficult even for a careful reader to deduce the practical implications of their terms of service. This inaccessibility, in turn, discourages users from reading the terms at all.

The potential breadth of Facebook's Data Policy, for example, was laid bare in October 2014, when the company published a paper revealing that it had been "experimenting" on how slight changes to the site could impact on users' political engagement or mood.[26] The idea of a formal experiment on 61 million unsuspecting subjects raised concerns, particularly in light of the potential for large-scale social manipulation. The company defended the experiment in part by noting references to academic research in their Data Policy. Nonetheless, it is likely that, if users who signed up for a Facebook account were presented with a clear, bold message saying that the company intended to use them to carry out social and behavioural experiments, at least a few may have reconsidered.

This is not to minimise the legitimate challenges that intermediaries face in engaging users on these issues, and the difficulty of reducing a document that has legal implications to simple, user-friendly terms. Nonetheless, more needs to be done to ensure that terms of service and other polices are clear. The increasing publication of "simplified" terms is a good start, though these must be crafted carefully to avoid painting an inaccurate picture. Recent years have also seen independent initiatives aimed at enhancing user understanding of intermediaries' policies, which intermediaries should support.[27]

Consultation is also important and intermediaries should consult with users prior to making major amendments to their terms of service, notify users of any amendments they do make and make previous versions available so that users can understand the changes. Ideally, outreach should go even further, including by providing avenues of engagement for users seeking clarification of their terms of service or other policy questions, and by allowing users to propose policy changes.

Responding to State Attacks on Freedom of Expression

Many intermediaries face the challenge of what to do when confronted by government demands which do not accord with international human rights standards. The responsibility to avoid complicity in human rights violations is a key

[26] Micah L. Sifry, "Facebook Wants You to Vote on Tuesday. Here's How It Messed With Your Feed in 2012", Mother Jones, 31 October 2014. Available at: www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout.
[27] An example of this is "Terms of Service; Didn't Read". Available at: tosdr.org/.

part of the UN's Protect, Respect and Remedy framework,[28] as well as the main focus of the GNI.

Some of the most challenging cases of private sector complicity in human rights violations involve China, which has not only demanded compliance with invasive censorship demands but also sought to enlist private sector collaboration in persecuting prominent critics, and even in supporting State cyber attacks.[29] The country has been particularly bold in taking action against companies that refuse to acquiesce to their demands, including by blocking them from the lucrative Chinese market. Although China is the most high profile and extreme example, companies face similar dilemmas in other countries, including sometimes in developed democracies.

No government, of course, has a perfect human rights record. What constitutes a legitimate restriction on freedom of expression is a complex question and different countries have different rules. By and large, it is reasonable to expect intermediaries to comply with local laws on these issues in the jurisdictions where they operate. But more active steps to avoid complicity in human rights abuses are warranted when operating in countries with poor human rights records.

Intermediaries should carefully assess the risks whenever a new potentially risky market is entered or a new product is launched, and develop strategies to mitigate these, for example by disabling features which may be prone to misuse in a particular national context or by avoiding locating their employees or storing data in countries which have a poor record of respecting human rights. Most global tech companies only maintain a physical presence in a few countries, and other States have no real legal means to compel compliance with their demands, other than by threatening to deny the company access to their market. Being shut out of a country is obviously not a consequence to be taken lightly, given the commercial implications. However, if the major players put up a unified front in support of human rights, it will be difficult for countries to ban them all (although China may represent an exception here).

Intermediaries will need to consider carefully whether a violation is significant enough to warrant noncompliance with domestic law. Although the line can be difficult to draw, where an intermediary encounters a case of their systems or services being subverted to support a clear and grave violation of human rights, they have a responsibility to take action to avoid or mitigate complicity. This can include refusing to turn over records that support a political prosecution or to participate in widespread systems of repression, such as China's Great Firewall.

---

[28] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, 7 April 2008. Available at: www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-report-7-Apr-2008.pdf.

[29] Bill Marczak and Nicholas Weaver, "China's Great Cannon", Munk School of Global Affairs, 10 April 2015. Available at: citizenlab.org/2015/04/chinas-great-cannon/.

Relevant considerations here include the number of users impacted, the severity of the interference and the broader human rights context in which the interference takes place, including the country's overall human rights record.

Where a State-mandated interference falls short of a clear and grave violation of human rights, intermediaries should only hand over information when subject to a legal requirement to do so and should notify users who are subject to a government request as soon as this is legally allowed. Where realistic legal avenues for contesting problematic laws or policies exist, intermediaries have some responsibility to launch legal challenges in appropriate cases and to stand up for the rights of their users. Intermediaries should also explore their options for seeking external leverage, such as soliciting diplomatic support from supportive governments or from intergovernmental organisations, and to liaise with one another to establish a unified front.

Introduction

At the height of its power, the British East India Company ruled over a population of 90 million people, in an area larger than the United Kingdom, through the might of its own 200,000 strong standing army.[30] The Company waged wars, collected taxes, minted coins and, although nominally subject to the British crown, exercised virtually absolute authority over the areas it governed. This state of affairs lasted for over a century until, faced with a major revolt in India and increasing criticism over how a commercial enterprise could justify wielding this level of power and autonomy, the administrative duties of the Company were taken over by the British government in 1857, leading to the Company's eventual dissolution in 1874.

Although no modern corporation wages wars or levies taxes, recent years have seen the formation of new private sector empires in the online world that are, in terms of the overall power they wield, in some ways analogous to the East India Company. In an age of information, tech giants like Google, Facebook and Twitter hold unprecedented power over how people access information and communicate. In an increasingly large part of the world, the Internet is rapidly becoming the dominant mode of communication and the main means by which people not only socialise and entertain themselves but also engage politically and professionally.

Like the British East India Company, these online behemoths have benefitted by being at the vanguard of a new international economy. The online world is naturally borderless, making it an ideal environment for companies to expand globally. However, their rapid expansion is also due to the unique nature of the Internet and digital commerce, which requires vastly less physical infrastructure, and therefore allows an unprecedented level of scalability. Facebook was only founded 12 years ago and yet today the service has 1.44 billion monthly active users, one-fifth of the world's population.[31]

There are, of course, important differences between the East India Company and today's tech giants. The success of these modern entrepreneurs is something to be welcomed and applauded. They earned their position by developing new and innovative products. Their businesses support the spread of the Internet, making it more accessible, functional and user-friendly by facilitating the ability of users to find information, translate websites, engage in commerce and communicate with their friends. At the same time, as the Internet expands and more of our lives move online, the level of control that private sector interests have over online communications has increasingly important implications.

---

[30] "The Company that ruled the waves", The Economist, 17 December 2015. Available at: www.economist.com/node/21541753.

[31] Emil Protalinsky, "Facebook passes 1.44B monthly active users and 1.25B mobile users; 65% are now daily users", Venture Beat, 22 April 2015. Available at: venturebeat.com/2015/04/22/facebook-passes-1-44b-monthly-active-users-1-25b-mobile-users-and-936-million-daily-users.

As a result of the nature of the digital world, regulatory gaps and the technical sophistication of the tools required to communicate online – tools which are invariably developed, distributed and controlled by the private sector – the private sector has become a major mediator of online speech. No major tech firm exercises the level of power that the East India Company did. However, these firms make decisions which can dramatically impact the lives of hundreds of millions of people and set the tone for global conversations. Sometimes, their approach is developed at the behest and with the cooperation of public authorities, or through multi-stakeholder collaboration.[32] In other cases, their approach to regulating speech or protecting user privacy is formulated entirely on their own. Sometimes, companies engage in consultations with their users, or the public at large, to develop their policies and practices. Sometimes they do not. Sometimes their policies and practices are clear and unequivocal and distributed openly. Sometimes they are kept secret, or drafted in a manner which is vague or misleading.

The Internet's rapid rise has left regulators scrambling to keep pace. Many legal concepts that were developed in a pre-Internet era, such as copyright rules, are poorly suited to the digital age. It has been a challenge to update legislation to deal with the rapidly changing digital world and, at times, these efforts have been counterproductive. Recent years have seen a host of legislative proposals that were developed without a proper understanding of how the Internet works, for example by criminalising wide swaths of harmless or innocuous behaviour.[33]

The dissolution of the East India Company served to clarify the distinction between the role of States and the role of private sector actors. With the growing power of private sector intermediaries over the digital realm, and the enormous impact of their policies and practices on the exercise of key rights like freedom of expression and the right to political participation, traditional understandings of the role of the private sector need, once again, to be reconsidered.

This Report explores the role of private sector online intermediaries, which we define as private sector bodies whose online operations facilitate communication between two or more parties over the Internet. The Report begins by examining the role of the Internet as a key delivery mechanism for human rights and how human rights should be understood in an online context. It then discusses the responsibilities of private sector actors when it comes to safeguarding human rights, before examining a number of initiatives to promote human rights responsible conduct by online intermediaries.

---

[32] Amar Toor, "Facebook will work with Germany to combat anti-refugee hate speech", The Verge, 15 September 2015. Available at: www.theverge.com/2015/9/15/9329119/facebook-germany-hate-speech-xenophobia-migrant-refugee.

[33] See, for example, the Centre for Law and Democracy's analysis of Pakistan's proposed Prevention of Electronic Crimes Act (2014). Available at: www.law-democracy.org/live/wp-content/uploads/2014/03/Pak.Cyber_.Mar141.pdf.

The main part of the Report explores six specific themes of relevance to this issue, namely expanding access, net neutrality, moderation of content, privacy, transparency and responding to State attacks on freedom of expression. For each of these thematic sections, the Report maps the key areas where private sector policy or practice impacts on human rights and reviews better, and sometimes less salutary, practice among online intermediaries. These sections all finish with a set of recommendations for good practice among intermediaries.

It is well established that States bear primary responsibility for ensuring respect for human rights. Furthermore, the policies and practices of private sector online intermediaries can be heavily influenced by State policies and actions. Intermediaries must, for example, respect national laws in the countries in which they operate and they need to take into account the situations in which they may be exposed to liability for the actions of their users. However, State obligations are not the focus on this Report, and its recommendations are addressed exclusively to the question how private online intermediaries can and should behave.

Background Issues

Human Rights and the Internet

As an increasing proportion of our lives move online, the Internet has become a central feature in terms of promoting respect for human rights. An important starting point for any discussion about human rights and the Internet is that human rights standards apply to the online world. In June 2012, the UN Human Rights Council said that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights".[34] The UN General Assembly affirmed this in a 2013 resolution.[35]

The Internet also supports the promotion and protection of a number of human rights, most obviously freedom of expression but also the rights to association, to education, to work and to take part in cultural life, among others. The tremendous potential of the Internet as a force for development and the promotion of human rights was noted by the Inter-American Commission on Human Rights as early as 1999:

> [The Internet] is a mechanism capable of strengthening the democratic system, contributing towards the economic development of the countries of the region, and strengthening the full exercise of freedom of expression. Internet is an unprecedented technology in the history of communications that facilitates rapid transmission and access to a multiple and varied universal data network, maximizes the active participation of citizens through Internet use, contributes to the full political, social, cultural and economic development of nations, thereby strengthening democratic society. In turn, the Internet has the potential to be an ally in the promotion and dissemination of human rights and democratic ideals and a very important instrument for activating human rights organizations, since its speed and amplitude allow it to send and receive information immediately, which affects the fundamental rights of individuals in different parts of the world.[36]

These predictions of the Internet's importance in terms of human rights have been borne out in practice. In 2013, Navi Pillay, then the UN High Commissioner for

---

[34] Resolution A/HRC/20/L.13, 29 June 2012. Available at: www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc.

[35] Resolution A/C.3/68/L.45/Rev.1, 26 November 2013. Available at: www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1.

[36] *Annual Report of the Inter-American Commission on Human Rights 1999: Report of the Office of Special Rapporteur for Freedom of Expression*, 1999; Chapter II: Evaluation of the State of Freedom of Expression in the Hemisphere, Part D: The Internet and Freedom of Expression. Available at: www.summit-americas.org/Human%20Rights/Freedom-Expression-1999.htm.

Human Rights, commented on the Internet's transformative impact on the promotion of human rights:

> Modern technologies are transforming the way we do human rights work. In 1993, the World Wide Web was just four years old, and its future use and reach could barely have been imagined, nor how fundamentally the Internet would affect our lives. Together with social media and IT innovations, these technologies are dramatically improving real-time communications and information-sharing. They are also magnifying the voice of human rights defenders, shining a light on abuses, and mobilizing support for various causes in many parts of the world.[37]

The Internet's importance to human rights has led to calls for access to the Internet itself to be considered a human right.[38] Among the earliest statements in support of this can be found in Greece's Constitution, as amended in 2001, which stated in part:

> All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State… [39]

Using similar language, the Constitution of the Mexican state of Colima protects access to the information society.[40] In 2000, Estonia's parliament passed a law declaring that Internet access was a fundamental human right of citizens.[41] A right of access to the Internet, along with a concomitant duty on the State to promote and guarantee access, was also recognised by Costa Rica's Constitutional Court in a 2010 ruling.[42] An increasing number of jurisdictions impose universal service obligations on Internet access providers including Finland,[43] Spain[44] and the Canadian province of Nova Scotia.[45]

---

[37] Navi Pillay, United Nations High Commissioner for Human Rights, 20-20 Human Rights Vision Statement for Human Rights Day, 10 December 2013. Available at: www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14074.

[38] Centre for Law and Democracy, *A Truly World-Wide Web: Assessing the Internet from the Perspective of Human Rights* (Halifax: Centre for Law and Democracy, 2012). Available at: www.law-democracy.org/wp-content/uploads/2010/07/final-Internet.pdf.

[39] Article 5A(2). Available at: www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf.

[40] Article 1(IV). Available [in Spanish] at: info4.juridicas.unam.mx/adprojus/leg/7/218/.

[41] Colin Woodard, "Estonia, where being wired is a human right", Christian Science Monitor, 1 July 2003. Available at: www.csmonitor.com/2003/0701/p07s01-woeu.html.

[42] Sentencia 12790: Expediente: 09-013141-0007-CO, para. V. Available [in Spanish] at: 200.91.68.20/pj/scij/busqueda/jurisprudencia/jur_repartidor.asp?param1=TSS&nValor1=1&nValor2=483874&strTipM=T&lResultado=1&pgn=&pgrt=&param2=1&nTermino=&nTesauro=&tem1=&tem4=&strLib=&spe=&strTem=&strDirTe.

[43] Communications Market Act, 363/2011, s. 60C(2). Available at: www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf.

[44] Sustainable Economy Act of 2011, Article 52. Available [in Spanish] at www.boe.es/boe/dias/2011/03/05/pdfs/BOE-A-2011-4117.pdf.

[45] Michael MacDonald, "Eastlink gets rural broadband deadline", Canadian Press, 20 February 2014. Available at: www.cbc.ca/news/canada/nova-scotia/eastlink-gets-rural-broadband-deadline-1.2545211.

Tamir Israel

Most states in the Western European and Others (WEOG) region recognize a legal Universal Service obligation in positive law, while a few others address Universal Service considerations as a non-binding but important government policy objective.[46] A growing number of WEOG states are recognizing narrowband and broadband connectivity as 'essential communication' that attracts the Universal Service obligation, while others are actively considering taking such a step.[47] Eight EU states have, for example, extended their respective national service obligations to include broadband and a ninth has included accessibility obligations for those with disabilities.[48] The European Commission is currently considering including broadband explicitly within its EU-wide Universal service regime, whereas the United States has already done so. Many other States are mobilising ancillary state initiatives outside of (but often strongly analogous to) the Universal Service obligation in order to advance towards universal adoption of broadband connectivity.[49]

However, Universal *access* to infrastructure alone does not achieve the Universal Service objective in and of itself, which aims at universal *adoption*. As most WEOG region Universal Service objectives are realized in an environment characterized by some level of market competition, the Universal Service obligation will typically include criteria aimed at ensuring that essential communications are not only available to all, but available at an affordable price.[50] Cost ceilings are viewed as necessary to spurring universal *adoption* by normalizing what would otherwise be excessive retail costs arising from high infrastructure construction in rural areas, or even as a means of ensuring essential services are rendered affordable to segments of the population that could otherwise not afford them.[51]

---

[46] Mexico, for example, is a rare OECD country that does not recognize Universal Service as a legal obligation in national law: OECD, "Universal Service Policies in the Context of national Broadband Plans", July 25, 2012, DSTI/ICCP/CISP(2011)10/FINAL, Annex – Country Examples; Eli Noam, "Beyond Liberalization III: Reforming Universal Service", http://www.citi.columbia.edu/elinoam/articles/beyondlib3.htm, "Universal service goals exist in every developed country. This suggests that similar benefits for a widespread interconnectivity are perceived around the world, usually independently of the political party in power."

[47] BEREC, BoR(14)95, p 6.

[48] BEREC, BoR(14)95, p 41.

[49] OECD, "Universal Service Policies in the Context of national Broadband Plans", July 25, 2012, DSTI/ICCP/CISP(2011)10/FINAL, generally.

[50] OECD, "Universal Service Obligations in a Competitive Telecommunications Environment", (1995) *Committee on Information, Communications and Computers Policy* No 38, p 5, defines the Universal Service obligation as an obligation "to provide basic telephone service to all who request it at a uniform price even though there may be significant differences in the costs of supply".

[51] OECD, "Universal Service Policies in the Context of national Broadband Plans", July 25, 2012, DSTI/ICCP/CISP(2011)10/FINAL, p 9.

The 2011 *Joint Declaration on Freedom of Expression and the Internet* by the special international mandates for freedom of expression[52] also highlighted States' duty to promote universal access to the Internet:

> Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet. Access to the Internet is also necessary to promote respect for other rights, such as the rights to education, health care and work, the right to assembly and association, and the right to free elections.[53]

While the right to freedom of expression has long been understood to impose a positive obligation on States to promote a robust expressive environment,[54] it is relatively novel for access to a particular technology or means of communication to be considered a human right. The recognition noted above therefore signals the radical and transformative potential of the Internet as a communicative medium. Furthermore, a significant groundswell of support underlies this position. A BBC World Service poll in 2010 found that 79 percent of people around the world believe that access to the Internet is a fundamental right.[55]

The Internet's Impact on Freedom of Expression and Privacy

The growth of the Internet and its centrality to many aspects of modern life is starting to impact on our understanding of certain rights. Of particular note here is the evolving dynamic between the right to privacy and the right to freedom of expression.

The nexus between these rights predates the digital age. The right to privacy has long been understood as including a right to secrecy of correspondence, and control over one's communications is a vital aspect of freedom of expression.[56] On the other hand, there are also areas where privacy interests conflict with freedom of expression or vice versa, such as in the context of media reporting on someone's private affairs. In these cases, the conflict is generally resolved by assessing whether the overall public interest supports privacy or publication of the information.

---

[52] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the 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. Since 1999, these mechanisms have adopted a Joint Declaration annually focusing on a different freedom of expression theme.

[53] 1 June 2011. Available at: www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.

[54] See, for example, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27, para. 66. Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[55] See: "Internet access is 'a fundamental right'", BBC, 8 March 2010. Available at: news.bbc.co.uk/1/hi/technology/8548190.stm.

[56] Shawn Powers, "Where did the principle of secrecy in correspondence go?", The Guardian, 12 August 2015. Available at: www.theguardian.com/technology/2015/aug/12/where-did-the-principle-of-secrecy-in-correspondence-go.

The rise of the Internet has impacted significantly on this balancing by expanding the expressive sphere, often at the expense of traditional notions of privacy. Due to the ubiquity of digital technologies, people are choosing to share more information about themselves than ever before. This explosion in the distribution and collection of personal information is compounded by the permanence and accessibility of online information. Shared information can become indelibly attached to a person, following them for years or decades, by which time it has become misleading or irrelevant. This information is also vastly more accessible online than when stored in other formats. Evidence of a speeding ticket incurred by a young person, once available only to those who searched through official records or a public library holding the newspaper where this information had been published, is now retrievable through a simple search on their name. Furthermore, although users are choosing to share more personal information, a significant volume of the personal information which is collected and shared is done so without the meaningful consent of the data subject, either because he or she does not fully understand the tools being used or because the information is posted by third parties.

In addition, the collection and commercialisation of user information is now used to support many of the "free" products and services available online. As a result, moves to protect privacy online often not only restrict speech directly, by limiting what a particular party can share or communicate, but also pose a risk to online speech more broadly, by threatening the commercial viability of the tools through which mass communication is achieved. The Internet has thus raised the stakes in traditional conflicts between freedom of expression and privacy by facilitating enormous expressive benefits based on an economic model which seriously undermines privacy.

Human Rights and the Private Sector

Horizontal Application of Rights

The challenge of establishing an appropriate balance between freedom of expression and privacy on the Internet is further complicated by the fact that the tools which facilitate online speech are generally owned and operated by private sector actors. International human rights rules are primarily designed to bind the actions of States rather than private actors. The former are obliged to serve the interests of their people. They are also granted a monopoly on powers such as the use of force and the right to imprison, powers that must be constrained to prevent abuse. By contrast, corporations operate with more limited power, and are expected to pursue their own interests, potentially even if these do not align with the general public interest. Corporations are also subject to regulation by States, reinforcing the latter's status as the primary duty bearer for safeguarding human rights.

Human rights obligations, as applied to States, impose positive as well as negative obligations. International human rights law requires States to take positive action to ensure that people can enjoy and exercise their rights, including when the threat to those rights comes from the private sector, sometimes referred to as the horizontal application of rights. For freedom of expression, there is an obligation to take positive measures to secure the free flow of information and ideas in society:

> [T]he State may be required to put in place positive measures to ensure that its own actions contribute to the free flow of information and ideas in society, what may be termed 'direct' positive measures. This might involve, for example, putting in place a system for licensing broadcasters which helps ensure diversity and limit media concentration. Perhaps the most significant example of this is the relatively recent recognition of the obligation of States to put in place a legal framework to provide for access to information held by public bodies. [references omitted][57]

Part of this positive obligation includes passing laws to prevent rights violations by third parties. A good example of this is the adoption of hate speech laws, required by Article 20(2) of the *International Covenant on Civil and Political Rights* (ICCPR).[58] States are also arguably under an obligation to adopt other laws restricting freedom of expression, including privacy and defamation laws.

Despite this, there are many reasons why intrusive government regulation of the online world is not a desirable solution from a human rights perspective, including to ensure that online discourse maintains its open and freewheeling character. However, if private sector actors adopt policies or practices which unduly interfere with either the flow of information or privacy, or fail to put in place policies which facilitate a strong expressive environment, an argument could be made for a stronger State role. This thinking, and the implicit threat of State intervention, has been in the background of previous debates about human rights and the private sector. During the early discussions over forming the Global Network Initiative (GNI), an international partnership which aims to improve human rights among private sector online intermediaries, a high ranking United States Senator said that if "U.S. companies are unwilling to take reasonable steps to protect human rights, Congress must step in."[59] This factor can both lead to a direct impact (i.e. where regulatory measures are imposed) and to an indirect impact, insofar as it encourages the private sector to take the initiative to improve their human rights footprint.

There are also cases where States have imposed positive human rights responsibilities on the private sector. For example, it is accepted better practice for

---

[57] Toby Mendel, *Restricting Freedom of Expression: Standards and Principles* (Halifax: Centre for Law and Democracy, 2011). Available at: www.law-democracy.org/wp-content/uploads/2010/07/10.03.Paper-on-Restrictions-on-FOE.pdf.
[58] UN General Assembly Resolution 2200A(XXI), 16 December 1966, in force 23 March 1976.
[59] Larry Downes, "Why no one will join the Global Network Initiative", Forbes, 30 March 2011. Available at: www.forbes.com/sites/larrydownes/2011/03/30/why-no-one-will-join-the-global-network-initiative/.

right to information laws to apply to private sector bodies which either receive public funding or perform a public function, to the extent of that funding or function.[60] The African Commission on Human and Peoples' Rights' Model Law on Access to Information goes even further, imposing a responsibility on all private sector bodies to respond to right to information requests if the information may assist in the exercise or protection of any right.[61]

Guidelines for Human Rights in the Private Sector

With the rise of the Internet, major mechanisms for facilitating both speech and surveillance are now under the control of private sector online intermediaries. Increasingly, State actors have come to rely on private sector online intermediaries to facilitate their work, either by removing content posted by their users or by gathering and handing over information about them. As such, companies often function as intermediaries between citizens and governments, putting them in prime position to facilitate, or push back against, abusive State conduct. Indeed, in some instances private sector information gathering systems have driven the capabilities of government surveillance forward, as technologies developed by the private sector for commercial purposes have been integrated into State intelligence and law enforcement systems.

Over the past two decades, there have been increasing moves to recognise that the private sector has a direct responsibility – whether of a legal or moral nature – to respect human rights. Although much of the initial support behind this idea originated with particularly heinous violations committed by companies in the garment and extractive industries, private sector online intermediaries' unique gatekeeper role for the exercise of human rights has also made them a major focus.

The most high profile work in this regard has been developed by Harvard Professor John Ruggie, who was appointed in 2005 as the Special Representative of the Secretary-General on human rights and transnational corporations and other business enterprises. After three years of extensive research and consultations with governments, business and civil society, the Special Representative presented the "Protect, Respect and Remedy" framework[62] to the Human Rights Council, which unanimously welcomed the document.

The basic idea underlying the Protect, Respect and Remedy framework is that States have an obligation to prevent human rights abuses by third parties, while private

[60] Centre for Law and Democracy and Access Info Europe, "RTI legislation Rating Methodology", 29 September 2012, Available at: www.law-democracy.org/wp-content/uploads/2011/09/Indicatorsfinal.pdf.
[61] Section 2(b). Available at: www.achpr.org/files/news/2013/04/d84/model_law.pdf.
[62] Human Rights Council, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, 7 April 2008, A/HRC/8/5. Available at: www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-report-7-Apr-2008.pdf.

entities have a responsibility to respect human rights and act with due diligence to avoid infringing the rights of others, and that victims of rights abuses deserve access to effective remedies, both judicial and non-judicial. Although the Protect, Respect and Remedy framework focuses on doing no harm, it also notes that this "is not merely a passive responsibility for firms but may entail positive steps – for example, a workplace anti-discrimination policy might require the company to adopt specific recruitment and training programmes."[63]

Moreover, the Protect, Respect and Remedy framework acknowledges that it is only a conceptual starting point:

> Governments have adopted a variety of measures, albeit gingerly to date, to promote a corporate culture respectful of human rights. Fragments of international institutional provisions exist with similar aims.
> …
> The United Nations is not a centralized command-and-control system that can impose its will on the world – indeed it has no "will" apart from that with which Member States endow it. But it can and must lead intellectually and by setting expectations and aspirations.[64]

Following the acceptance of the Protect, Respect and Remedy framework, the Human Rights Council extended Ruggie's mandate to develop the concepts into concrete recommendations. This resulted, in 2011, in the *Guiding Principles on Business and Human Rights,* which include the following statement:

> The responsibility to respect human rights is a global standard of expected conduct for all business enterprises wherever they operate. It exists independently of States' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations. And it exists over and above compliance with national laws and regulations protecting human rights… Business enterprises may undertake other commitments or activities to support and promote human rights, which may contribute to the enjoyment of rights. But this does not offset a failure to respect human rights throughout their operations.[65]

The Organisation for Economic Co-operation and Development's (OECD) *Guidelines for Multinational Enterprises* also notes that private sector actors have their own responsibilities in terms of complying with human rights rules and that non-compliance by the States in which they operate does not relieve them of these responsibilities:

> A State's failure either to enforce relevant domestic laws, or to implement international human rights obligations or the fact that it may act contrary to such laws or international obligations does not diminish the expectation that enterprises respect human rights. In countries where domestic laws and regulations conflict

[63] *Ibid.,* para. 55.
[64] *Ibid*., para. 105-107.
[65] UN OHCHR, Guiding Principles On Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, 16 June 2011, HR/PUB/11/04, p. 14. Available at: www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

> with internationally recognized human rights, enterprises should seek ways to honour them to the fullest extent which does not place them in violation of domestic law.[66]

In September 2015, Maina Kiai, the UN Special Rapporteur on the rights to freedom of peaceful assembly and association, called for a binding international treaty imposing human rights responsibilities on businesses. Speaking in the context of the trade in natural resources, Kiai noted that a major difficulty in guaranteeing human rights stemmed from the enormous power exercised by corporations:

> [T]here are voluntary principles, such as the UN Guiding Principles on Business and Human Rights, but these rely on commitments from individual companies and place no legal requirement for corporations to redress human rights violations. As a result, these commitments are often just window dressing. This means states alone must enforce domestic laws on human rights norms – an outcome that is not guaranteed once business gets involved, particularly with large and influential corporations.[67]

Corporate Social Responsibility

It is accepted that corporations have certain responsibilities to behave in socially positive ways, sometimes referred to as corporate social responsibility. The importance of this is increasingly being recognised by private sector intermediaries. For example, in August 2014, a series of sexually explicit photographs of celebrities, which were illicitly obtained through hacks of their iCloud accounts, were leaked online. Reddit, a website whose users played a key role in the photos' distribution, received a lot of criticism in the aftermath of the event. A few days later, in a blog post entitled "Every Man is Responsible for His Own Soul", the website disavowed any responsibility to police their users. At the same time, the administrators noted:

> [W]e consider ourselves not just a company running a website where one can post links and discuss them, but the government of a new type of community. The role and responsibility of a government differs from that of a private corporation, in that it exercises restraint in the usage of its powers.[68]

As noted already, there are major differences between a government and a private corporation, which this quote from Reddit's administrators does not necessarily take fully into account. However, as the quote illustrates, private sector intermediaries are increasingly recognising that the power they have over communication in the online world comes with some responsibilities. However, even if one assumes maximum goodwill on the part of the private sector, corporate responsibility is tricky to define. In some cases an ethical policy will make business sense, but there are certainly areas where human rights conflict with the profit

---

[66] OECD, Guidelines for Multinational Enterprises, 2011. Available at: mneguidelines.oecd.org/text/.
[67] Maina Kiai, "A binding international instrument on business & human rights should safeguard civic space", 2015. Available at: business-humanrights.org/en/a-binding-international-instrument-on-business-human-rights-should-safeguard-civic-space.
[68] Reddit, "Every Man Is Responsible For His Own Soul", 6 September 2014. Available at: www.redditblog.com/2014/09/every-man-is-responsible-for-his-own.html.

motive, leading to questions as to what should reasonably be expected from private sector actors and what does it mean for a company to act in a manner which aligns with human rights standards.

It can be argued that a strong approach to safeguarding human rights is in the interest of online intermediaries. Widespread access to the Internet, with the communications power that this grants to everyday users, has led to an increase in public pressure on corporations to be seen to be acting as a force for good. Where consumers can choose their digital providers, or where corporations are publicly traded, this creates a commercial incentive for companies to act in socially responsible ways:

> There is growing evidence that good practice: enhances reputation, resulting in improved staff morale, leading to higher motivation, productivity, and the ability to attract and retain the best employees; strengthens the licence to operate, giving improved access to new markets, consumers and investors; creates more stable operating environments; and promotes better community relations. Conversely, companies implicated in human rights scandals often see their reputations and brand images suffer, resulting in the loss of share value, and face increased security and insurance costs, as well as expensive lawsuits, such as those pursued under the US Alien Tort Claims Act, and consumer boycotts. The price of getting it wrong cannot be underestimated. … Human rights are basic standards aimed at securing dignity and equality for all. International human rights laws constitute the most universally accepted standards for such treatment … International consensus has been achieved on what constitutes human rights in the form of the 1948 Universal Declaration of Human Rights (UDHR).[69]

Similarly, the UN Global Compact highlights why it is in companies' interests to support human rights:

> Respect for human rights is the right thing to do, but it is also a business issue. Not respecting human rights poses a number of risks and costs for business including putting the company's social license to operate at risk, reputational damage, consumer boycotts, exposure to legal liability and adverse government action, adverse action by investors and business partners, reduced productivity and morale of employees.[70]

Sensitivity among private sector players regarding how they are perceived has been amplified due to the fact that the Internet has made it increasingly difficult to keep secrets from one's customers, as well as from civil society observers. For example, while the connections between major tech firms and the United States' National Security Agency (NSA) remained hidden for a period of time, eventually word leaked, creating a public relations disaster for the companies involved.

---

[69] Castan Centre for Human Rights Law, *International Business Leaders Forum and Office of the United Nations High Commissioner for Human Rights, Human Rights Translated – A Business Reference Guide* (2008). Available at: www2.ohchr.org/english/issues/globalization/business/docs/Human_Rights_Translated_web.pdf.

[70] United Nations Global Compact, "The Ten Principles of the UN Global Compact". Available at: www.unglobalcompact.org/what-is-gc/mission/principles/principle-1.

Freedom of Expression, Privacy and Intermediaries

As noted earlier, a key challenge to guaranteeing freedom of expression on the Internet is the role that private sector online intermediaries play in providing access to, managing, facilitating and mediating online speech. This is due partly to the sophisticated technical and infrastructural requirements involved in connecting to and taking advantage of digital possibilities, partly to the trans-national nature of the Internet and partly to the dynamic role these private sector intermediaries have played in the development of the World Wide Web.

Private sector companies have always been highly influential expressive actors. Newspapers are generally owned by private individuals or corporations, as are the majority of broadcasters and other mass communication platforms. What is different in the context of the Internet is that private sector intermediaries facilitate speech directly by individuals. Rather than creating a platform for an influential few, as newspapers or broadcasters do, the Internet's power is that it gives everyone a platform, and potentially a global audience.

On 2 May 2011, when the United States military launched its raid against Osama bin Laden in Abbottabad, Pakistan, a local resident named Sohaib Athar live-tweeted the events as he saw them outside of his window.[71] In a pre-digital world, Mr. Athar may have chatted about what he saw to a neighbour or possibly to a visiting journalist in the days to come. Thanks to Twitter, he ended up providing the world with its first reporting of the events. Among the triggers of the 2011 Tahrir Square protests which brought down long-standing Egyptian President Hosni Mubarak was a video posted to Facebook by 26-year-old activist Asmaa Mahfouz, saying she planned to hold up a banner in the square and exhorting others to join her.[72]

Tools like Twitter and Facebook allow ordinary speakers to reach an audience of potentially millions. While this is an incredible benefit, the fact that private sector actors control these primary outlets for self-expression also means that their policies and practices can be very significant for free speech online.

The Internet has also led to traditionally public avenues for expression being replaced by private services. The postal service, for example, has since its earliest inception been organised and operated in most places by governments. However, it is rapidly being supplanted by email, which is largely controlled by the private

---

[71] Mike Butcher, "Here's the guy who unwittingly live-tweeted the raid on Bin Laden", TechCrunch, 2 May 20111. Available at: www.techcrunch.com/2011/05/02/heres-the-guy-who-unwittingly-live-tweeted-the-raid-on-bin-laden-2/.

[72] "Asmaa Mahfouz & the YouTube Video that Helped Spark the Egyptian Uprising", Democracy Now, 8 February 2011. Available at: www.democracynow.org/2011/2/8/asmaa_mahfouz_the_youtube_video_that.

sector. In 2014, postal services around the world processed just under 400 billion pieces of mail,[73] roughly equivalent to the volume of emails which are sent every two days.[74] While most progressive governments have specific rules regarding how mail is handled, including with regard to the privacy of correspondence, in the private sector rules are much less clearly defined. The expansion of the private sector into these areas has been accompanied by new pressure from States for companies to facilitate human rights violations, such as through participating in intrusive surveillance systems or acting to police user content.

These potential dangers was noted in the 2011 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression:

> Given that Internet services are run and maintained by private companies, the private sector has gained unprecedented influence over individuals' right to freedom of expression and access to information. Generally, companies have played an extremely positive role in facilitating the exercise of the right to freedom of opinion and expression. At the same time, given the pressure exerted upon them by States, coupled with the fact that their primary motive is to generate profit rather than to respect human rights, preventing the private sector from assisting or being complicit in human rights violations of States is essential to guarantee the right to freedom of expression.[75]

In June 2009, in the midst of major demonstrations in Iran against an unpopular election result, Twitter opted to delay scheduled maintenance of its servers so as to avoid interfering with communications by protestors, who had come to rely on the service.[76] In contrast to its supportive attitude towards the Iranian demonstrators, in April 2015 the service announced that it had suspended approximately 10,000 accounts associated with the militant Islamic State.[77] In both cases, it is difficult to fault Twitter for choosing the side that it did. However, the fact that the service is choosing sides raises important questions about the power and influence that it, and other major intermediaries, wield.

In 2013, Facebook faced controversy after removing pages linked to the Peace and Democracy Party (BDP), then Turkey's largest pro-Kurdish political party. Facebook stated that the removals were linked to posting of content in support of the

---

[73] United States Postal Service, Size and Scope, Available at: about.usps.com/who-we-are/postal-facts/size-scope.htm.

[74] Sara Radicati, Email Statistics Report 2014-2018 (April 2014). Available at: www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf.

[75] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27 (16 May 2011), para. 44. Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[76] Evgeny Morozov, "Iran Elections: A Twitter Revolution?", Washington Post, 17 June 2009. Available at: www.washingtonpost.com/wp-dyn/content/discussion/2009/06/17/DI2009061702232.html.

[77] Rick Gladstone, "Twitter Says It Suspended 10,000 ISIS-Linked Accounts in One Day", New York Times, 9 April 2015. Available at: www.nytimes.com/2015/04/10/world/middleeast/twitter-says-it-suspended-10000-isis-linked-accounts-in-one-day.html.

Kurdistan Workers' Party (PKK), which violated their prohibition on expressing support for internationally-recognised illegal terrorist organisations.[78] While some States, including the United States, where Facebook is based, have labelled the PKK a terrorist group, others have refused to do so.

While, strictly speaking, each intermediary only exercises control over its own platform, the dominant market position a small number of major players hold, particularly in emerging online markets, means that their decisions can decisively impact broader online expression. In Myanmar, for example, Facebook is by far the dominant social network.[79] A decision by the company to restrict a particular type of content there can make it vastly more difficult for a user to get their message out.

Beyond decisions over content moderation, subtle changes in how content is presented by online intermediaries can have a dramatic impact on users' behaviour. In the 2010 US election, Facebook tweaked its newsfeed for certain users in a manner which encouraged voter turnout, which was credited with having a significant impact on whether or not they voted.[80] Although the changes were apparently made on an apolitical basis, some expressed unease over the potential for "digital gerrymandering" and the idea that private sector intermediaries could use their power to drive turnout or support to a particular party or candidate.[81] The solution, according to Jack Balkin of Yale Law School and Jonathan Zittrain of Harvard Law School, is for these private sector intermediaries to be considered as "information fiduciaries", which engages responsibilities not to use information management tools to further ideological goals and to keep automatically generated records of when the personal data of their users is shared with another company:

> Constructed correctly, the duties of the information fiduciary would be limited enough for the Facebooks and Googles of the world, while meaningful enough to the people who rely on the services, that the intermediaries could be induced to opt into them. To provide further incentive, the government could offer tax breaks or certain legal immunities for those willing to step up toward an enhanced duty to their users.[82]

Fostering Respect for Human Rights among Private Sector Online Intermediaries

The Global Network Initiative

---

[78] Facebook censorship of pro-Kurdish political party", Deutsche Welle, 2 November 2013. Available at: www.dw.com/en/facebook-censorship-of-pro-kurdish-political-party/a-17199752.
[79] On Device Research, "Myanmar: the final frontier for the mobile internet", 23 June 2014. Available at: ondeviceresearch.com/blog/myanmar-mobile-internet-report.
[80] Bond, R. M., *et al.*, "A 61-million-person experiment in social influence and political mobilization" (2012) 489 Nature, pp. 295-298.
[81] Jonathan Zittrain, "Facebook Could Decide an Election Without Anyone Ever Finding Out", New Republic, 1 June 2014. Available at: newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.
[82] *Ibid.*

The most prominent initiative thus far aimed specifically at improving the conduct of private sector online intermediaries is the Global Network Initiative (GNI).[83] The GNI was launched in 2008 through the combined efforts of leading academics and civil society organisations as well as representatives from major players in the tech sector. The signatory companies agreed to follow the GNI's Principles on Freedom of Expression and Privacy (the GNI Principles),[84] and subject themselves to regular assessments of their compliance.

Although the GNI was able to sign up some of the world's largest and most influential ICT companies, it has also faced criticisms, mainly that the GNI Principles and their enforcement mechanisms are too soft and flexible to guarantee good conduct effectively. Amnesty International refused to sign on for that reason, although they released a statement upon the GNI's launch recognising that it was a step forward.[85] Reporters Without Borders also declined to sign on, expressing concern about "loopholes and weak language on the central principles that may threaten the very implementation of these principles and justify the status quo."[86] The weakness of the standards was even tacitly acknowledged by some of the GNI's chief participants. For example, Nicole Wong, Google's Deputy General Counsel responsible for privacy, noted: "The GNI principles are broad enough to support our policies in China, both before and after we changed our approach in the country."[87] This is a surprising admission, given that much of the original impetus for the GNI came from criticisms about United States tech firms' collaboration with the Chinese government.

Some consider these criticisms of the GNI to have been vindicated by the 2013 Snowden disclosures, which revealed the involvement of GNI members in mass surveillance efforts by the United States National Security Agency (NSA), as this type of behaviour was precisely what the GNI was designed to mitigate. The revelations led the Electronic Frontiers Foundation, a high profile GNI civil society participant, to withdraw from the process.[88] In some cases, companies are legally prohibited from discussing their interactions with United States intelligence gathering by gag orders. However, the companies themselves have also imposed limits on the GNI's ability to gather complete information. For example, in their first round of

[83] See: www.globalnetworkinitiative.org.
[84] Available at: globalnetworkinitiative.org/principles/index.php.
[85] Bobbie Johnson, "Amnesty criticizes Global Network Initiative for online freedom of speech", The Guardian, 30 October 2008. Available at: www.theguardian.com/technology/2008/oct/30/amnesty-global-network-initiative.
[86] Reporters Without Borders, "Why reporters without borders is not endorsing the global principles on freedom of expression and privacy for ICT companies operating in internet-restricting countries", 28 October 2008. Available at: en.rsf.org/why-reporters-without-borders-is-28-10-2008,29117.html.
[87] Larry Downes, "Why no one will join the Global Network Initiative", Forbes, 30 March 2011. Available at: www.forbes.com/sites/larrydownes/2011/03/30/why-no-one-will-join-the-global-network-initiative/.
[88] Jillian York, "EFF Resigns from Global Network Initiative", Electronic Frontier Foundation, 10 October 2013. Available at: www.eff.org/press/releases/eff-resigns-global-network-initiative.

assessments, released in 2014, the GNI notes that assessors were limited in their ability to access information protected by solicitor-client privilege.[89] The rules on solicitor-client privilege can be waived at the discretion of the client, in this case the company, which was free to share the information with the GNI assessors had they wished to do so.

A lack of transparency in the GNI assessment process is another concern, since currently assessments only present results through aggregated findings and a few anonymised cases. In other words, particular problematic (or exemplary) conduct which the assessment unearths is not publicly attributed to any specific company.

It is, however, worth noting that the GNI retains many high profile members, such as Human Rights Watch and the Berkman Center for Internet & Society at Harvard University, which defend the GNI as an important mechanism for facilitating dialogue between the private sector and the human rights community, and for promoting the spread of good practices among its private sector membership. The GNI operates in a very difficult field, where compliance is necessarily voluntary. The broader challenges in promoting good practice among private sector intermediaries, which can generally be expected to pursue their own interests rather than acting for the public good, may necessitate compromises. The GNI also helps to fill an important regulatory gap, particularly in assessing whether a company's public statements match its actual performance. Moreover, the GNI claims that its assessments have raised awareness of the importance of human rights among their private sector members significantly, have expanded the use of human rights impact assessments (HRIAs) in advance of key policy changes (the GNI provides guidelines on how to carry out a strong HRIA), and have in particular increased consideration of human rights among senior management.

Although the GNI provides valuable guidance in the areas that it deals with, there are important policy and practice areas that are outside of this focus. The preamble to the GNI Principles states broadly that, "ICT companies have the responsibility to respect and protect the freedom of expression and privacy rights of their users". However, the action areas that follow focus almost exclusively on guarding against government interferences. For freedom of expression, this means:

> Participating companies will respect and protect the freedom of expression of their users by seeking to avoid or minimize the impact of government restrictions on freedom of expression, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication.
>
> Participating companies will respect and protect the freedom of expression rights of their users when confronted with government demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to

[89] Global Network Initiative, "Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo", January 2014. Available at: globalnetworkinitiative.org/sites/default/files/GNI Assessments Public Report.pdf.

> information and ideas in a manner inconsistent with internationally recognized laws and standards.[90]

The freedom of expression section of the GNI Implementation Guidelines, which provides practical guidance on how to put the GNI Principles into practice, is wholly focused on interactions with government, with no consideration of the impact of a company's policies beyond this.[91] On privacy, there is some mention of direct private sector responsibility in the GNI Principles, but this is case in vague terms and is relatively permissive in nature.

The GNI assessments, which measure how the GNI Principles have been applied in practice by member companies, further attest to this focus. The 2014 *Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo* lists seven issues which are considered to be part of the process, six of which are wholly concerned with how members react to State interferences.[92] The seventh, content surveillance, could potentially encompass independent private sector action as well, although there is no indication in the findings that this was considered. Of the nine illustrative case studies listed in the Report, eight deal with government requests to access or remove information, although the ninth relates to employee access to user data.

The GNI's focus on government interferences is not surprising given that, as discussed above, traditional views about human rights obligations have tended to focus on the State. However, there remains a significant need for policy guidance of the ethical responsibilities of private sector intermediaries beyond how they interact with abusive requests from States.

Other Initiatives

In recent years, there has been an increasing focus on the human rights implications of private sector activities beyond how they respond to government abuses. In June 2013, the European Commission published a guiding document to help companies in the ICT sector fulfil their responsibilities under the UN's *Guiding Principles on Business and Human Rights*.[93] This focuses mainly on responding to harmful State policies or requests, but it also provides guidance on better practice for protecting user privacy more generally, as well as how to communicate clearly with users, including through terms of service.

---

[90] See footnote 49.
[91] *Ibid*.
[92] Available at: globalnetworkinitiative.org/sites/default/files/GNI Assessments Public Report.pdf.
[93] The Institute for Human Rights and Business and Shift, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights", European Commission, June 2013. Available at: ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf.

In 2014, UNESCO released *Fostering Freedom Online: The Role of Internet Intermediaries*, which provides recommendations for private sector conduct, including the following: "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."[94]

Within civil society, there has also been an increasing focus on the need to promote good practice in the private sector. Particularly notable in this area is the Ranking Digital Rights Project, whose Corporate Accountability Index evaluates 16 of the world's most powerful Internet and telecommunications companies based on 31 indicators.[95] The Corporate Accountability Index covers some of the same ground as the GNI, such as whether companies communicate clearly with their users and carry out human rights impact assessments. However, it digs more deeply into companies' policies, including assessing their level of transparency and due process in removing content or restricting accounts, their network management policies and their data security standards. This represents a significant step forward conceptually, and the Ranking Digital Rights Project is currently working to expand the Index further.

Another project of note is the *Manila Principles on Intermediary Liability*, which were developed by a coalition of civil society groups and which focus on obligations and responsibilities of both States and private sector intermediaries regarding takedown requests and the disclosure of user information.[96]

Dialogue on this issue is also moving forward through the Dynamic Coalition on Platform Responsibility (DCPR), which in 2015 unveiled a set of Recommendations on Terms of Service and Human Rights. The DCPR is a multi-stakeholder platform which meets every year at the Internet Governance Forum and facilitates ongoing conversations through their online mailing list.[97]

Conclusion

Promoting human rights at the State level is by no means a simple task, but efforts to promote respect for human rights among private online intermediaries are, in many ways, more complicated and challenging. Human rights principles, as well as

---

[94] UNESCO, "Fostering Freedom Online: The Role of Internet Intermediaries", 2014. Available at: unesdoc.unesco.org/images/0023/002311/231162e.pdf.
[95] Rebecca Mackinnon, "The Ranking Digital Rights 2015 Corporate Accountability Index is now online!", Ranking Digital Rights, 3 November 2015. Available at: rankingdigitalrights.org/.
[96] 24 March 2015. Available at: www.manilaprinciples.org.
[97] Internet Governance Forum, "Dynamic Coalition on Platform Responsibility (DC PR)". Available at: www.intgovforum.org/cms/2008-igf-hyderabad/event-reports/74-dynamic-coalitions/1625-dynamic-coalition-on-platform-responsibility-dc-pr. The Recommendations are available at: review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-platform-responsibility-dc-pr/. The Coalition's own website is available at: platformresponsibility.info/.

the mechanisms to enforce them, were generally designed for States. Furthermore, solidarity from States in promoting respect by other States is common, whether conducted on a bilateral basis or through intergovernmental organisations. It is common for democratic countries to pressure dictatorships to reform and to refuse to do business with those which refuse to. This dynamic does not translate to companies, whose relationships are inherently more competitive and adversarial. Governments are also naturally expected to be open and transparent, whereas corporations have much more legitimate expectations of secrecy for their operations. A model of information being open by default, which progressive States are embracing, would be almost unthinkable in a private sector context.

There are, as a consequence, three layered challenges which any initiative to promote good practice in the private sector faces. The first is engagement, simply getting major private sector interests to the table. The second is transparency, in terms of getting access to internal information in order to conduct assessments and then being open about the results of those assessments. The third is actually fostering change: convincing companies to amend policies or practices which are problematic. Internal compromises may be needed to limit these challenges. For example, an initiative may sacrifice transparency in terms of assessment results in order to obtain access to the internal information needed to conduct the assessment, or it may create a weaker compliance mechanism so as to get major players to the table.

These are significant challenges but the human rights community must address them if it is to promote greater respect for human rights by corporations. Although this is a field which is still in its infancy, the importance of the private sector to guaranteeing respect for human rights, and in particular of private sector online intermediaries to guaranteeing freedom of expression and privacy, requires continued focus and engagement in order to promote positive change.

Key Issues: Expanding Access

As a practical matter, promoting human rights on the Internet means expanding access, so that the benefits conferred may be enjoyed as widely as possible. Furthermore, access to the Internet is increasingly being recognised as a human right.[98] Although the past decades have seen a rapid increase in the number of people who use the Internet, important access gaps have also emerged. According to the International Telecommunication Union (ITU), globally the total number of people using the Internet as of the end of 2015 was 3.2 billion, of whom 2 billion were from the developing world. However, another 4 billion people, mostly from developing countries, remain offline. Of the 940 million people living in the least developed countries (LDCs), only 89 million, less than 10 percent, use the Internet. This may be contrasted with an overall penetration rate of 80 percent in the developed world.[99]

The gap between wealthy and poor countries is not the only divide. There is also a gap between urban and rural access, which is evident across both the developed and developing world. According to a 2010 census, 12.7 percent of urban dwellers in Ghana used the Internet compared with only 2.1 percent of rural dwellers.[100] In 2012, a study found that 17.3 percent of urban Ugandans had used the Internet at least once in the preceding 3 months, as compared to 6.5 percent of rural Ugandans,[101] while in India, the figures are 64 percent compared to just 9 percent.[102] According to the Canadian Internet Registration Authority, broadband connections are technically available to 100 percent of Canadians who live in urban areas, while in rural areas the figure is 85 percent.[103] A study by the Pew Research Center found that 85 percent of urban adult citizens in the United States were

---

[98] See, for example, the Joint Declaration on Freedom of Expression and the Internet, adopted by the special international mandates on freedom of expression on 1 June 2011. Available at: www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.

[99] Brahima Sanou, ICT Facts & Figures (May 2015: International Telecommunication Union (ITU) Telecommunication Development Bureau). Available at: www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

[100] Alliance for Affordable Internet (A4AI), Affordable Internet In Ghana: The Status Quo and the Path Ahead (2014). Available at: a4ai.org/wp-content/uploads/2014/03/Ghana-Case-Study-Layout-Final.pdf.

[101] Alliance for Affordable Internet (A4AI), Affordability Report (2015). Available at: 1e8q3q16vyc81g8l3h3md6q5f5e.wpengine.netdna-cdn.com/wp-content/uploads/2015/03/a4ai-affordability-report-2014.pdf. In Mozambique, the figure in urban areas was 26 percent, compared to 3.2 percent rurally.

[102] Darrell M. West, "Digital divide: Improving Internet access in the developing world through affordable services and diverse content", Center for Technology Innovation at Brookings, February 2015. Available at: www.brookings.edu/~/media/research/files/papers/2015/02/13%20digital%20divide%20developing%20world%20west/west_internet%20access.

[103] Canadian Internet Registration Authority, The Canadian Internet (2014). Available at: cira.ca/factbook/2014/the-canadian-internet.html.

classed as Internet users in 2015, compared with 78 percent of rural adult citizens.[104]

Various factors contribute to both discrepancies. Infrastructure challenges and costs are often significant and may be compounded in the developing world by the absence of a reliable power grid. Urban areas are smaller and hence easier to connect, and provide a higher density of prospective users, so they generally represent more economically lucrative targets for commercial access providers. Mobile Internet sites are also two to three times cheaper to build in urban areas as compared to rural ones.[105] Put differently, it is more expensive to provide access to sparsely populated rural areas and these costs must be borne by a smaller base of customers, making it more expensive to connect rural areas.[106]

Landlocked countries also face challenges in connecting their people. Because major backbone connections tend to run under the ocean, landlocked countries can be at the mercy of their neighbours in terms of access. Across Africa, Internet penetration rates among the 16 landlocked countries average 13 percent, compared with an overall Internet penetration rate of 33 percent for the coastal countries.[107] According to statistics from the ITU, prices for fixed broadband service, as assessed against purchasing power parity (PPP) are nearly four times higher in landlocked African countries than among the continent's coastal nations.[108]

In developing countries as a whole, average monthly mobile broadband prices, as assessed using PPP, are twice as expensive as in developed countries, while fixed broadband prices are three times higher.[109] This impacts on urban-rural differentials since most of the world's poor live in rural areas.[110] In the United States, median household income for urban areas was USD 52,988 in 2012,

---

[104] Andrew Perrin and Maeve Duggan, Americans' Internet Access: 2000-2015, Pew Research Center, 26 June 2015. Available at: www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/. As of December 2013, 79 percent of urban Australians had an Internet connection in their home, as compared to 72 percent of rural Australians. Australian Communications and Media Authority, Regional Australia in the digital economy, 14 August 2014. Available at: www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Research-snapshots/Regional-Australia-in-the-digital-economy.

[105] Facebook, "State of Connectivity 2015: A Report on Global Internet Access", 21 February 2016. Available at: newsroom.fb.com/news/2016/02/state-of-connectivity-2015-a-report-on-global-internet-access/.

[106] Jon Brodkin, "Man builds house, then finds out cable Internet will cost $117,000" Ars Technica, 30 September 2015. Available at: arstechnica.com/business/2015/09/man-builds-house-then-finds-out-cable-internet-will-cost-117000/.

[107] Statistics from www.internetworldstats.com/stats1.htm. Estimates are from 30 June 2015.

[108] International Telecommunication Union, "Measuring the Information Society Report, 2015", (Geneva: ITU, 2015). Available at: www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf.

[109] Brahima Sanou, note 99.

[110] Alain de Janvry, Rinku Murgai, and Elisabeth Sadoulet, "Rural Development and Rural Policy", University of California at Berkeley, June 1999. Available at: are.berkeley.edu/~esadoulet/papers/Handbook_text.pdf.

compared to USD 41,198 in rural areas.[111] Across the European Union, the greatest share of population at risk of poverty is in thinly populated rural areas.[112]

The challenges of expanding rural access to the Internet were noted in a report by the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in 2011:

> Internet access is likely to be concentrated among socioeconomic elites, particularly in countries where Internet penetration is low. In addition, people in rural areas are often confronted with obstacles to Internet access, such as lack of technological availability, slower Internet connection, and/or higher costs. Furthermore, even where Internet connection is available, disadvantaged groups, such as persons with disabilities and persons belonging to minority groups, often face barriers to accessing the Internet in a way that is meaningful, relevant and useful to them in their daily lives.[113]

As the Special Rapporteur notes, costs are only one part of the problem. A lack of demand can also inhibit the Internet's spread. Demand challenges can, among other things, be linguistic or social in nature. There are more than 6,900 different languages in the world, about 400 of which have at least one million speakers.[114] However, while the World Wide Web abounds in content written in English, Spanish and Russian, far less material is available in less widely spoken languages.

A lack of relevant content, for example of a political, economic or cultural nature, or the absence of a significant number of users from a person's community to interact with, can similarly depress demand, since the utility of the Internet to a given individual depends in important ways on one's ability to connect with a relevant community. Disability can exacerbate other barriers to accessing the Internet, and marginalised groups in general are under-represented online. In developing countries, women are 25 percent less likely to be online than men.[115]

It is worth noting that these various infrastructural, economic and social challenges can be mutually reinforcing. Just as infrastructure challenges can drive up the cost of access by forcing ISPs to pay more to connect users, high access costs depress demand, further driving up per capita infrastructure costs. Low demand, in turn,

---

[111] United States Department of Agriculture, Rural America at a glance (2014). Available at: www.ers.usda.gov/media/1697681/eb26.pdf.
[112] European Commission Agriculture and Rural Development, EU Agricultural Economic briefs (May 2011). Available at: ec.europa.eu/agriculture/rural-area-economics/briefs/pdf/01_en.pdf.
[113] United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27. Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[114] Darrell M. West, "Digital divide: Improving Internet access in the developing world through affordable services and diverse content", Center for Technology Innovation at Brookings, February 2015. Available at: www.brookings.edu/~/media/research/files/papers/2015/02/13%20digital%20divide%20developing%20world%20west/west_internet%20access.
[115] *Ibid.*

limits the development of culturally relevant content from underserved areas, further reducing the incentive for these users to get online.

Regulatory obstacles can also inhibit the expansion of Internet access. These can be overtly designed to limit the spread of the Internet, for example where there is official suspicion of its potential use to support activism and political mobilisation, but more often they are the result of a lack of understanding of the mechanics of how the Internet works. For example, laws are often proposed which would impose licensing obligations on various sorts of Internet services, without taking into account that these are completely different in nature from the offline models that regulators are basing the licensing rules on.

Although problematic legislation is, of course, an issue for which governments, rather than the private sector, bears primary responsibility, private sector players can play an important positive role in helping to overcome this.

Free Internet and Progressive Pricing

The most obvious area where private sector actors facilitate the spread of Internet access is through programmes to provide free access to new users. Some of these projects are remarkably ambitious. Google and Facebook have announced projects to connect rural users through high altitude balloons and solar-powered aircraft, respectively.[116] Pricing is a major area where private sector policies can have an impact on the spread of the Internet. While it is understandable that ISPs might wish to charge more to rural customers, reflecting the higher costs associated with this, these pricing differences exacerbate the existing digital divide.

From a human rights perspective, better practice would be to minimise, or ideally to eliminate, pricing differential based on location. In some places, government programmes or regulations harmonise prices between urban and rural users. For example, the Broadband for Rural Nova Scotia initiative was a public-private partnership that required broadband access to be provided to any household that requested it at the same monthly cost being paid by urban customers.[117] Other governments offer grants or loans to extend access to rural households or impose regulatory regimes which effectively require urban customers to subsidise rural

[116] See: Project Loon, available at: www.google.com/loon/; and Yael Maguire, "Building communications networks in the stratosphere", Code Facebook, 30 July 2015, available at: code.facebook.com/posts/993520160679028/building-communications-networks-in-the-stratosphere/.

[117] Motorola, "The Fastest Province in Canada" (2008). Available at: www.motowirelessnetwork.com/pdf/sm_vertical_market_segment_sales_tools/carrier_wisp/Case%20Study_Nova%20Scotia%20Project.pdf.

access.[118] Even where these arrangements are not in place, access providers should consider adopting pricing schemes which render Internet access affordable for all potential users and which extend access as widely as possible. This responsibility is particularly acute where a company has a monopoly in a particular region, so that a decision not to provide access to certain users or to price a connection beyond what residents can afford effectively denies them access. In order to further ease the economic challenges that underlie the digital divide, companies could also consider offering subsidised Internet to poor households.

Where economic pressures against universal service are particularly challenging, cost saving measures such as providing slower or capped access for rural users are preferable to not providing access at all. A slow or capped connection still delivers most of the Internet's core benefits, including social communication, political engagement, access to news and information, and most forms of telecommuting. Bandwidth-intensive services like video streaming are popular, but if there really is a need to choose between pricing Internet access beyond generally affordable levels, or offering slower or capped service, the latter are clearly preferable.

Tamir Israel

As the variety of essential (or 'near essential) communications networks evolve, states employ a more complex range of strategies with the objective of maximizing connectivity, each envisioning differing roles and obligations for the intermediary service providers involved. Australia's National Broadband Network (NBN), for example, sought to build a national high speed fibre (or near-fibre) network with public revenues, and to then grant commercial service providers access to this network, in effect elevating the quality of all domestic networks in ways that would not have been achieved by commercial parties alone.[119] In reviewing its Universal Service obligation the Canadian Radio-television and Telecommunications Commission (CRTC) chose to announce targets of 5 / 1 Mbps downstream / upstream that it expected to be made available in all rural areas. While not a strict regulatory obligation imposed on any service provider, the CRTC clearly indicated that it would monitor the realization of

[118] United States Department of Agriculture, USDA Announces Funding for Rural Broadband Projects (20 July 2015). Available at: www.usda.gov/wps/portal/usda/usdahome?contentid=2015/07/0212.xml.

[119] OECD, "The Development of Fixed Broadband Networks", January 8, 2015, DSTI/ICCP/CSIP(2013)8/FINAL, pp 24-25; The scope of this obligation was narrowed somewhat following: National Broadband Network, "Strategic Review – December 2013", Final Report. A number of EU states also employ public funding schemes outside the scope of the Universal Service obligation as a means of facilitating broadband growth: BEREC, BoR(14)95, p 43. The European Commission has allocated 500 million Euros to fund broadband deployment projects within the European Union: Robert Viola, "500 Million € for Broadband Projects – Fund Manager Needed", June 13, 2016, *European Commission: Digital Single Market*, https://ec.europa.eu/digital-single-market/en/blog/500-million-eu-broadband-projects-fund-manager-needed.

these targets with the expectation that if they were not met within a given timeframe, heavier regulatory tools would be employed.[120]

As a final example, the United States Federal Communications Commission (FCC) established a "Connect America Fund" drawn from the existing Universal Service Fund and dedicated to broadband deployment. As an initial condition, Fund recipients were obligated to deploy broadband networks capable of supporting at least 10 / 1 Mbps residential connectivity.[121] The Fund itself is comprised of mandatory annual donations from service provider non-rural revenues, creating a subsidization mechanism overseen by the FCC.[122] It is therefore not dependent on direct government investment from general revenues, but does allow for such investment to enhance infrastructure development timelines or to compliment infrastructure development schedules in other ways.[123] More recently, the FCC recognized that higher quality broadband (25 / 3 Mbps) was required and not being universally provided in a sufficiently timely manner by current levels of private and public investment.[124] It is currently examining ways to best achieve this higher level of connectivity.[125]

---

[120] Canada, CRTC, Telecom Regulatory Policy CRTC 2011-291, *Obligation to serve and other matters*, May 3, 2011, File Nos: 8663-C12-201000653, 8663-C12-200912437 & 8663-C12-200909658. The European Union adopted a similar EU-wide target approach, set to achieve basic broadband access for everyone by 2013, and at least 30 Mbps coverage for 100% of European Union citizens coupled with at least 50% of households adopting 100 Mbps connections by 2020. These targets are monitored by Eurostat: European Commission, "A Digital Agenda for Europe", May 19, 2010, COM(2010)245 Final and OECD, "National Broadband Plans", June 15, 2011, DSTI/ICCP/CISP(2010)9/FINAL), p 16.

[121] United States, Federal Communications Commission, *In Re: Inquiry Concerning Deployment of Advanced Telecommunications Capability*, FCC-15-10A1, paras 143-145.

[122] https://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db1211/DOC-330989A1.pdf

[123] https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-190A1_Rcd.pdf. As noted above, 8 EU states also impose explicit narrowband or broadband connectivity obligations in their national legal or regulatory regimes: BEREC, BoR(14)95, pp 39-42.

[124] United States, Federal Communications Commission, *In Re: Inquiry Concerning Deployment of Advanced Telecommunications Capability*, FCC-15-10A1.

[125] *Ibid*. The European Commission has also recently completed a consultation in order to determine how to address EU broadband requirements past 2020: EC, "Public Consultation on the Needs for Internet Speed and Quality Beyond 2020", September 11, 2015, https://ec.europa.eu/digital-single-market/en/news/public-consultation-needs-internet-speed-and-quality-beyond-2020#EN. The consultation has ended, and the Commission is now preparing a report that will establish the next stage of its regulatory approach to broadband: EC, "Contributions and Preliminary Trends of the Public Consultation on the Needs for Internet Speed and Quality Beyond 2020", March 3, 2016, https://ec.europa.eu/digital-single-market/en/news/contributions-and-preliminary-trends-public-consultation-needs-internet-speed-and-quality.

Promoting Demand

In addition to keeping costs of access down, intermediaries can play an important role in breaking down other barriers to access. This is a responsibility which will mainly fall on content and software providers, rather than access providers. In terms of accessibility measures, the World Wide Web Consortium's Web Content Accessibility Guidelines are an excellent starting point for facilitating access for the disabled.[126] Popular content providers and software developers should work to expand accessibility for underserved communities, for example by translating their platforms or content into new languages. According to the Broadband Commission for Digital Development's 2015 report, only 5 percent of the world's languages (by number of languages) are currently present on the Internet.[127] Major international actors, including Facebook and Google, should treat this as a priority, since they often serve as gatekeepers for vast stores of online content.

Cutting Off Access

State-mandated measures to cut off or deny service to users are considered highly intrusive from a freedom of expression perspective and are almost never justified according to international human rights law. International standards also hold that cutting off access to an entire population or segment of the public is never justified.[128]

Where a government demands that an access provider cut off or deny service to a user or group, this places the provider in a difficult position. They should resist these measures as far as possible, and not implement them unless confronted with a clear and binding legal instruction to do so. Even where a clear and binding legal instruction is in place, access providers should consider the broader human rights implications of their actions and whether there are viable alternatives. Options might include leaving the country or seeking external leverage to resist the request, such as through diplomatic support from their home government, as discussed in the section on Responding to State Attacks on Freedom of Expression. In addition, access providers should be transparent when asked to cut off access, including about having received the request and how they have responded, as part of their routine transparency systems. In all instances, access providers should push back against any orders to cut off access as far as possible, including by making use of any

[126] World Wide Web Consortium (W3C), Web Content Accessibility Guidelines 2.0, 11 December 2008. Available at: www.w3.org/TR/WCAG20/.
[127] "The State of Broadband 2015", UNESCO, 2015. Available at: www.broadbandcommission.org/documents/reports/bb-annualreport2015.pdf.
[128] See Joint Declaration on Freedom of Expression and the Internet, 1 June 2011. Available at: www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.

legal appeal mechanisms. Beyond legal requirements, voluntary schemes to cut off access should be avoided by access providers.[129]

[129] Nate Anderson, "Major ISPs agree to "six strikes" copyright enforcement plan", Ars Technica, 7 July 2011. Available at: arstechnica.com/tech-policy/2011/07/major-isps-agree-to-six-strikes-copyright-enforcement-plan/.

Stand Up For Digital Rights

Recommendations for Expanding Access:

Infrastructure:

- **Internet access providers should invest a reasonable proportion of their profits in expanding the infrastructure for providing access to the Internet, particularly so as to reach underserved communities, including potentially through entering into public-private partnerships to advance this goal.**

Cost Measures:

- **Internet access providers should consider funding or otherwise supporting programmes or schemes designed to support access for poorer households.**
- **Internet access providers should work to mitigate or eliminate pricing differentials between rural and urban customers.**

Promoting Accessibility

- **Private sector online intermediaries (intermediaries) should promote the development of content of relevance to less connected communities and/or in smaller languages, and awareness raising in those communities and language groups about the potential of the Internet.**
- **Intermediaries should promote accessibility for the disabled by adopting the World Wide Web Consortium's Web Content Accessibility Guidelines.**

Other Issues:

- **Internet access providers should make reasonable efforts to monitor attempts by governments to adopt legislative rules which unduly undermine the expansion of access to the Internet and should engage in**

or support awareness raising and advocacy efforts to combat such moves.

- **Internet access providers should never acquiesce to an external request to cut off access or deny service to a user unless required to do so by a clear and binding legal order.**

Key Issues: Net Neutrality

As the Internet has grown, and become more lucrative, a debate has been taking place about the foundational principle of network neutrality, which means that Internet traffic should be treated equally, without any discrimination, restriction or interference based on the device, content, author, origin and/or destination of the content, service or application. Net neutrality prevents private sector intermediaries from favouring or disfavouring the transmission of certain types of Internet traffic.[130]

There are several reasons why net neutrality is fundamentally important. A commonly cited one is that it promotes free competition by preventing bigger players from abusing their position to obtain preferential access to customers. This also reflects concerns about the global digital divide, since allowing major firms to obtain preferential access would tip the balance in favour of early roll-out countries such as the United States and against emerging digital markets in the global south. Another benefit of net neutrality is that it limits the ability of private intermediaries to control the conversation that takes place over their networks, for example by blocking or slowing access to a website whose content they disagree with.

Centre for Internet and Society

The net neutrality debate across South Asia has largely focused on differential pricing and price discrimination. Price discrimination can be:

- Positive (sponsored data or zero rating): For example, an Internet service provider may favour an application, service or platform over others for a fee or a competitive advantage.
- Negative: For example, an Internet service provider may discriminate against a service or platform and the end user is implicitly or explicitly assessed an additional fee to access that service or platform.

Differential pricing is the practice of charging different consumers different prices for the same product, and can be based on services, content or application. Zero rating, where a service or content is offered for free or at a very low cost, is one type of differential pricing. There are a number of arrangements for zero rated services including:

- Subsidised: The ISP, the content provider, the government or another third party pays for a service to be offered at a subsidised rate.
- Negotiated: A third party, such as a content provider, enters into an

[130] There are recognised exceptions to this rule, such as where necessary to protect the integrity or security of a network or to combat spam. For a more thorough description, see: www.thisisnetneutrality.org/.

agreement with the ISP to have the service offered for free or at a lower rate.
- Mandated: The government requires a service to be zero rated.
- Self-imposed: An ISP selects which services to offer at lower rates or allows consumers to choose.

Such arrangements can zero rate based on content (including applications and platforms), services, protocols and carriers, or can be neutral with regard to content, service and carrier.

The reception, success and impact of zero rated services and can be both positive and negative and can be influenced by whether a company is foreign or local, the size of an ISP or the company offering a zero rated service, the specific market structure, the service that is zero rated, and the degree of Internet penetration in a specific context. For example, the Centre for Internet and Society and others have argued that when communication or publishing services are zero rated it can positively enable freedom of expression. Zero rating can also enable the right to access by reducing costs and can provide market advantage for services offering local content and services offering access to under served communities. At the same time, if not transparent and left unregulated, the impact of zero rated services can be harmful.

Net neutrality is among the Internet's most revered principles, as a reflection of the medium's underlying egalitarian nature and as a prerequisite for continued innovation. One of the reasons for the increase in debate about it is the rise of bandwidth-intensive activities, in particular streaming high-quality video, which can place a heavy burden on existing networks, requiring greater investment in new infrastructure, with access providers then looking for ways to cover the costs.

States have approached this issue in different ways. In the United States, net neutrality is governed by the Federal Communications Commission's (FCC) Open Internet rules, which prohibit Internet access providers from blocking access to legal content, applications, services or non-harmful devices, from impairing or degrading lawful Internet traffic on the basis of its content and from favouring some lawful Internet traffic over other lawful traffic in exchange for consideration, which effectively precludes access providers from prioritising their affiliates.[131]

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

The ultimate goal of net neutrality is to keep the architecture of the Internet as it was first conceived: as a highway on which information flows freely and equally, with no more intervention than is necessary to manage traffic flows. Of course, net

[131] Federal Communications Commission, Open Internet, 23 October 2015. Available at: https://www.fcc.gov/openinternet.

neutrality is not an end in itself but rather a response to the extraordinary usefulness of the Internet as a tool for freedom of expression and knowledge sharing. From a democratic point of view, allowing ISPs to block or discriminate between content would grant them a powerful weapon of censorship in the service of private interests. From an economic point of view, quasi-monopolistic situations would lead to rapid market concentration of communications and content.

The business context cannot be neglected in the discussion about net neutrality, specifically the merger between owners of telecommunications networks, owners of companies providing Internet services and owners of content. The adoption of net neutrality by the Federal Communications Commission (FCC) of the United States shows that regulation of anti-competitive behaviour lies at the core of the issue. Comcast, one of the largest Internet access providers in the country, was the first company to sue the FCC over its authority to impose net neutrality rules. This managed to delay the imposition of rules for a while. Years later, with the neutrality rules in place, Comcast was forced to stop a planned purchase of Time Warner Cable due to concern over the merger of the largest Internet service provider with the largest provider of cable. The merger of AT&T and DirectTV had better luck, notwithstanding the FCC-imposed condition that AT&T substantially extend access to the Internet and "refrain from imposing discriminatory usage-based allowances or other discriminatory retail terms and conditions on ITS broadband Internet service." This shows that net neutrality regulation and competition are two sides of the same coin, at least in the minds of the FCC Commissioners.

On 27 October 2015, the European Parliament approved their own set of net neutrality rules, which state in part:

> Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.[132]

Although the proposal appears to guarantee broadly net neutrality, critics have pointed to an exception for "specialised services" which could potentially be abused to circumvent the spirit of the rule, as well as the fact that zero rating systems are not expressly prohibited.[133]

---

[132] Council of the European Union, Regulation 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (25 November 2015). Available at: eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32015R2120.

[133] Jeremy Gillula and Jeremy Malcolm, "Closing the Loopholes in Europe's Net Neutrality Compromise", Electronic Frontier Foundation, 23 October 2015. Available at: www.eff.org/deeplinks/2015/10/closing-loopholes-europes-net-neutrality-compromise.

The Internet is constantly changing and there is no single and immutable rule for how networks should be managed. Access providers constantly face evolving challenges and threats. However, certain fundamental principles should guide their decision-making.

First and foremost, policies and technical protocols for managing Internet traffic should aim to improve the functioning of the Internet for all users. It is accepted that there is a need to manage the flow of information over the Internet in a smooth, efficient manner and traffic policies and technical protocols which aim to facilitate that will generally be legitimate, while those which provide other less public interest objectives may not.

Second, arrangements which favour traffic from or to users who pay a premium, or who have any sort of preferential or partnership arrangement with network managers, are unacceptable.

Third, transparency is very important. Access providers should be clear about any traffic or information management practices they employ. This should include publishing information about their policies and technical protocols for managing traffic, as well as periodic data summarising how traffic and information was handled over the preceding period, subject only to legitimate business confidentiality interests, such as to protect the efficacy of spam and malware mitigation techniques.

Fourth, where strong net neutrality principles are codified in law, access providers and other online service provides should respect the rules and avoid lobbying for change. Where the law is unclear or unsettled, they should act in a way that fully respects the principle of network neutrality.

Zero Rating

Probably the most contentious aspect of the debate over net neutrality concerns zero rating projects which are implemented to expand Internet access. Among the most well known of these is Free Basics, a Facebook-led initiative which essentially provides people with free access to a limited range of Internet services, notably a basic version of Facebook, along with weather reports, health information, Wikipedia, communication tools, and some news and other services via an app on mobile phones. According to its proponents, by offering users even a stripped-down version of the Internet for free, Free Basics is helping to generate interest among these users, who can then move on to paying for a full connection. The design of Free Basics also serves to expand Facebook's user base and to ensure that Facebook is central to these new users' understanding of the Internet. Although Free Basics is the most globally well known zero rating programme, many others are currently in operation.

Centre for Internet and Society

All of the service providers studied as part of our research have entered into partnerships with different companies to offer zero rated services, increased data capacities or reduced tariff services. Examples of the different services that have been adopted by the service providers which were studied include:

- Free Basics: This provides users with free access to a select set of websites as long as the user browses through the Free Basics platform or app. Free Basics also allows application developers to launch their applications on the Free Basics platform, and allows organisations to host their websites and services on the Free Basics platform as long as the application or website complies with Free Basics participation guidelines which include technical guidelines, legal terms, and a platform policy. Free Basics has positioned itself to the public as working towards bridging the digital divide and enabling digital empowerment. Free Basics is presently available in eleven Asia-Pacific countries, although it has been banned in India.
- Google Free Zone: In 2013, Airtel implemented a scheme called "Google Free Zone", whereby Google services were offered for free over its network. These services included Google Search, Gmail and Google Plus. Users could only access content linked on these pages and had to pay for any other links. The service was free as long as usage did not exceed 1GB per month.
- Wiki Zero: In 2015, GrameenPhone introduced zero rating services for Wikipedia in partnership with the Wikimedia Foundation for the purpose of developing more content in Bengali. Wikimedia Bangladesh and Grameenphone also provided training to students on how to edit Wikimedia.
- Equal Rating: GrameenPhone partnered with Mozilla in a collaborative effort to provide non-tiered and open access to the Internet. The model allows users to receive up to 20MB of unrestricted data per day, after watching a short ad in the phone's marketplace. This effort avoids zero rating any particular service.
- Airtel Zero: In 2015, Airtel introduced the platform Airtel Zero, which gave free access (zero rating) to a limited set of services curated by Airtel, including Flipkart and the Hike messaging service.
- Easy Net: In 2015, GrameenPhone introduced a programme which provided free video tutorials about the Internet as well as access to Facebook and Wikipedia on the GrameenPhone network. Consumers were also given the choice of purchasing small data packs without a subscription.

Since Free Basics was launched, it has expanded to 37 countries. It has also faced significant criticism for a few reasons. The main complaint is that the service

undermines the principle of net neutrality.[134] Free Basics has been ruled out by some regulatory agencies on these grounds. Opponents also claim that Free Basics undermines the development of the digital economy in poor countries by giving core apps away for free and that, rather than using Free Basics as an "on ramp" to the Internet, it creates a two-tiered system of Internet access whereby some sites can be accessed without charge while others require payment. Free Basics has also been criticised for privacy invasions by engaging participants in Facebook's system of generating revenue, which relies on selling otherwise private user information (although the app itself does not show ads and Facebook notes that access to Free Basics does not require a Facebook account).

On 24 September 2015, Facebook responded to criticism of Free Basics by implementing a number of changes, including expanding the programme to provide access to more websites and creating a platform for developers to submit content for inclusion.[135] Facebook also announced that it would support encrypted HTTPS services on both the Android app and the web version of Free Basics.

Centre for Internet and Society

The debates that have emerged in India, Singapore, and Bangladesh demonstrate that net neutrality impacts a number of issues – including access, privacy, competition, innovation, jurisdiction, and security – and that it is also raising larger questions about governance and the role of the private sector.

Mark Zuckerberg himself (perhaps unintentionally) began to touch on this when justifying Free Basics in an open letter, which stated: "We have collections of free basic books. They're called libraries. They don't contain every book, but they still provide a world of good. We have free basic healthcare. Public hospitals don't offer every treatment, but they still save lives. We have free basic education. Every child deserves to go to school. And in the 21st century, everyone also deserves access to the tools and information that can help them to achieve all those other public services, and all their fundamental social and economic rights." All of the services listed by Zuckerberg are services traditionally offered by governments.

As ICT companies become key delivery mechanisms for core rights, questions about the duty of these companies to be responsible and accountable for the rights of users become more relevant and important. More than ever companies need to be transparent and precise about their services and agreements, and to be willing to engage democratically with users and governments.

[134] The most energetic campaign against Free Basics has emerged in India under the banner "Save the Internet". A summary of their arguments against the programme is available at: blog.savetheinternet.in/what-facebook-wont-tell-you-about-freebasics/.
[135] "Update to Internet.org Free Basics", Facebook, 24 September 2015. Available at: https://info.internet.org/en/2015/09/24/update-to-internet-org-free-basic-services/.

Ideally, access schemes which are designed to get people online at a lower cost or for free should be designed and executed in a non-discriminatory manner. There is no question that zero-rating programmes which prioritise certain services violate net neutrality. There may, however, potentially be an argument that the harm inherent in these schemes is outweighed by their benefit in bringing new people online if these schemes are unequivocally shown to be more effective than other access options which respect net neutrality.

There is something to be said for the argument that even limited Internet access is better than nothing and for Free Basics' argument about an "on ramp" to spur demand for and interest in the Internet. However, as noted above, many projects exist which provide a similar "on ramp" to the Internet which do not compromise net neutrality, for example by offering Internet with a low data cap or other service limitations, raising questions about whether zero rating is necessary to bring people online. Aircel, an Indian mobile network operator, launched its own service in October 2015 called (somewhat confusingly) Free Basic Internet, which provides users with free access to the web at a slower speed for three months (or longer, if the users carry a specified monthly balance on their mobile account).[136] GrameenPhone, based in Bangladesh, grants users up to 20 MB of unrestricted data per day after watching a short advertisement.[137]

Facebook claims that Free Basics has brought over 25 million people online,[138] and that 50 percent of Free Basics users end up paying for Internet services beyond the limited free package that it provides within a month of signing up.[139] However, these statistics are impossible to verify and, anyway, offer only a partial picture of the service's overall impact. There is no telling whether, for example, Free Basics users who move to paying for Internet access continue to use Free Basics to connect to Facebook for free, or whether Free Basics' user base is really composed of new Internet users. Most important of all, there are no accurate statistics comparing the efficacy of Free Basics against "on ramp" programmes that respect net neutrality.

While we do not completely reject zero rating schemes, they inevitably fail to respect net neutrality principles and so they face a heavy burden of justification and proof that they serve the greater good. In particular, their operators should demonstrate that such programmes are clearly the most effective way to bring people online, and that the benefits are significant enough to justify making compromises to the principle of net neutrality. If this case can be made, the

---

[136] Shashidhar KJ, "Aircel to offer free Internet across India at 64 kbps", Medianama, 16 October 2015. Available at: www.medianama.com/2015/10/223-aircel-free-internet/.
[137] Nathan Eagle, "How To Make The Internet Free In Developing Countries", TechCrunch, 1 June 2015. Available at: techcrunch.com/2015/06/01/how-to-make-the-internet-truly-free-in-developing-countries/.
[138] Facebook, "Our Impact", available at: info.internet.org/en/impact/.
[139] Facebook, "Free Basics: Myths and Facts", 19 November 2015. Available at: https://info.internet.org/en/2015/11/19/internet-org-myths-and-facts/.

operators of zero rating schemes have a responsibility to work to mitigate their negative effects, such as by providing training for users in digital literacy and by actively working to educate users about the potential benefits of Internet access beyond the zero rated offerings.[140] In the case of Free Basics specifically, an additional problem is the pervasive confusion among millions of people between Facebook and the Internet and the fact that many people use Facebook without understanding that a broader Internet exists. This suggests that Facebook bears an even greater burden of justification for any zero rating it operates.[141]

[140] For a broader discussion of how specific zero rated plans should be assessed, see: Center for Democracy and Technology, "Zero Rating: A Framework for Assessing Benefits and Harms", January 2016. Available at: cdt.org/files/2016/01/CDT-Zero-Rating_Benefits-Harms5.pdf.

[141] Leo Mirani, "Millions of Facebook users have no idea they're using the internet", Quartz, 9 February 2015. Available at: qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/.

Stand Up For Digital Rights

Recommendations for Net Neutrality:

Supporting Net Neutrality:

- **Internet access providers should respect the principle of net neutrality, even when they are not required to do so by law. Among other things, this implies:**
  - **There should be no discrimination in the treatment of traffic across their networks and systems.**
  - **Their traffic management policies and technical protocols should be designed to promote objective traffic management goals.**
- **Internet access providers should be transparent about the traffic or information management policies and practices they employ, and provide detailed statistical information about how traffic and information is actually handled.**
- **Intermediaries should support and promote the idea of network neutrality and, at a minimum, never lobby against law reforms to the extent that those reforms promote this goal.**

Net Neutrality and Expanding Access:

- **Programmes to expand access to the Internet which offer a trade off in terms of services or connectivity should be designed in an open, non-exclusive, transparent manner which respects net neutrality and the right of users to choose what material they wish to access. For such programmes, the goal of giving the access provider a competitive advantage should not undermine the broader goal of connectivity.**
- **Programmes to expand access that employ zero rating (i.e. that provide free access to certain select applications or services) should be avoided unless it can be demonstrated clearly that these are significantly more effective than similar programmes which do not offend against net neutrality. Access providers which offer such programmes should make available information about their effectiveness for purposes of independent verification.**

Key Issues: Moderation and Removal of Content

Policy Measures by Intermediaries

Among the major factors behind the success of the Internet has been the open, honest and freewheeling nature of online discourse. Internet users who are connecting from the comfort of their home, and through the (perceived) anonymity of being behind a computer or mobile screen, feel comfortable sharing opinions and accessing information that they otherwise might not, due to official censorship or fear of legal or social reprisals. There is a brutal, no-holds-barred honesty to online speech that can be liberating and refreshing. However, this sense of anonymity, and the fact that online communications generally feel more remote than face-to-face communication, can also encourage people's darker impulses. The Internet provides a seemingly bottomless well of humour, storytelling and political commentary, but it is also a prime vehicle for vitriol and threats, as well as for the distribution of illegal material such as child sexual abuse imagery.

This dichotomy puts private sector intermediaries in a difficult position. On the one hand, for many the free flow of information is their bread and butter. Internet users, predictably, dislike having their thoughts and ideas controlled and have grown used to the freedom of being able to say whatever they like. Private sector intermediaries, as a consequence, have been keen to burnish their image as open and unfiltered platforms. Dick Costolo, a former CEO of Twitter, once described the company as being "the free speech wing of the free speech party."[142] In a post to the site's users, Reddit's then-CEO Yishan Wong said:

> We uphold the ideal of free speech on reddit as much as possible not because we are legally bound to, but because we believe that you – the user – has the right to choose between right and wrong, good and evil, and that it is *your responsibility* to do so. [emphasis in original][143]

At the same time, the growing influence of private sector intermediaries has placed them under increasing pressure to mitigate the less desirable aspects of online speech. This can include pressure from their own users, who may prefer an online experience which is free from abusive or offensive material. It is, in particular, no secret that the Internet can be an especially hostile place for women. On 24 September 2015, two prominent online figures, Anita Sarkeesian and Zoe Quinn, spoke at the United Nations about the threats and harassment they faced as part of 'GamerGate', a controversy over ethics in journalism related to video games that

[142] Emma Barnett, "Twitter chief: We will protect our users from Government", The Telegraph, 18 October 2011. Available at: www.telegraph.co.uk/technology/twitter/8833526/Twitter-chief-We-will-protect-our-users-from-Government.html.
[143] "Every Man Is Responsible For His Own Soul", Reddit, 6 September 2014. Available at: www.redditblog.com/2014/09/every-man-is-responsible-for-his-own.html.

spiralled into a campaign of anger against prominent women in the industry.[144] Both women were subjected to thousands of explicit rape and death threats and their personal contact information was widely disseminated. There were also attempts to steal or manipulate their online identities.[145]

While the experience of Anita Sarkeesian and Zoe Quinn was extreme, due to the fact that they were the public faces of a major conversation about sexism, harassment is a routine part of life for many women online. Caroline Criado-Perez, an activist who successfully lobbied to have Jane Austen replace Charles Darwin on the face of a British banknote, was similarly targeted with threats of death and rape.[146] In October 2015, Mia Matsumiya, a musician and blogger, started an Instagram account profiling the over one thousand abusive or sexually explicit messages she had received online over the period of a decade.[147] It is worth noting that Ms. Matsumiya is not a particularly prominent online figure and there is no reason to believe her experience was particularly exceptional. Writers at Jezebel, a feminist blog, have complained about visitors repeatedly and systematically posting images of violent pornography in the comment sections which follow their articles, which their staff must then sort through manually.[148] Although it is arguably the most pervasive "civility" issue on the Internet, gender-based harassment is part of a broader problem. Reddit, for example, contains dozens of forums dedicated to racial abuse, holocaust denial, pictures of dead children and many other forms of highly offensive content.

In response to these problems, there has in recent years been a trend towards more active content management by some major private sector intermediaries. However, this gives rise to tricky debates about when and how companies should intervene. It is conceptually easy to defend a laissez-faire approach, where companies only intervene when they are legally required to do so, on freedom of expression grounds. Once companies choose to go beyond that, the debate becomes far more tangled.

---

[144] A good summary of how this happened can be found in Jay Hathaway, "What Is Gamergate, and Why? An Explainer for Non-Geeks", Gawker, 10 October 2014. Available at: gawker.com/what-is-gamergate-and-why-an-explainer-for-non-geeks-1642909080.

[145] Jessica Valenti, "Anita Sarkeesian interview: 'The word "troll" feels too childish. This is abuse'", The Guardian, 29 August 2015. Available at: www.theguardian.com/technology/2015/aug/29/anita-sarkeesian-gamergate-interview-jessica-valenti.

[146] See: Katie Roiphe, "The Bank of England wanted to put Jane Austen on a 10-pound note. Then all hell broke loose. ", Slate, 6 August 2013, available at: www.slate.com/articles/double_x/roiphe/2013/08/the_anger_over_jane_austen_on_a_10_pound_note_proves_people_can_rage_over.html; and "Two jailed for Twitter abuse of feminist campaigner", The Guardian, 24 January 2014, available at: www.theguardian.com/uk-news/2014/jan/24/two-jailed-twitter-abuse-feminist-campaigner.

[147] Her account is available at: instagram.com/perv_magnet/.

[148] "We Have a Rape Gif Problem and Gawker Media Won't Do Anything About It", Jezebel, 11 August 2014. Available at: jezebel.com/we-have-a-rape-gif-problem-and-gawker-media-wont-do-any-1619384265.

A good example of these challenges came in the aftermath of the murder of journalist James Foley in August 2014. Foley was killed by the Islamic State, which then attempted to disseminate propaganda footage of the murder online. Twitter and YouTube, the two main platforms being used to share the material, moved swiftly to try and remove it from their networks and block users who uploaded, shared or linked to it. This muscular reaction resulted in at least some collateral damage against users who merely discussed or commented on the video. For example, Zaid Benjamin, a journalist who posted analysis and still images from the video, but not the moment of Foley's death or links to the video itself, had his account temporarily blocked. He reported that he lost 30,000 followers as a result.[149]

Although no sensible observer would fault Twitter or YouTube for attempting to remove graphic footage of a murder being disseminated as propaganda for a violent extremist group, some expressed unease at platforms with such a high level of power and influence exercising what is effectively editorial control over content being shared by their users. As James Ball, a writer for *The Guardian*, put it:

> Twitter, Facebook and Google have an astonishing, alarming degree of control over what information we can see or share, whether we're a media outlet or a regular user. We have handed them a huge degree of trust, which must be earned and re-earned on a regular basis.
>
> If Twitter has decided to make editorial decisions, even on a limited basis, it is vital that its criteria are clearly and openly stated in advance, and that they are consistently and evenly applied.[150]

Journalist Glenn Greenwald echoed these sentiments:

> [A]s a prudential matter, the private/public dichotomy is not as clean when it comes to tech giants that now control previously unthinkable amounts of global communications… These are far more than just ordinary private companies from whose services you can easily abstain if you dislike their policies. Their sheer vastness makes it extremely difficult, if not impossible, to avoid them… It's an imperfect analogy, but, given this extraordinary control over the means of global communication, Silicon Valley giants at this point are more akin to public utilities such as telephone companies than they are ordinary private companies when it comes to the dangers of suppressing ideas, groups and opinions. It's not hard to understand the dangers of allowing, say, AT&T or Verizon to decree that its phone

[149] Shane Harris, "Social Media Companies Scramble to Block Terrorist Video of Journalist's Murder", Foreign Policy, 19 August 2014. Available at: foreignpolicy.com/2014/08/20/social-media-companies-scramble-to-block-terrorist-video-of-journalists-murder/.

[150] James Ball, "Twitter: from free speech champion to selective censor?" The Guardian, 21 August 2014. Available at: www.theguardian.com/technology/2014/aug/21/twitter-free-speech-champion-selective-censor?CMP=twt_gu.

> lines may not be used by certain groups or to transmit certain ideas, and the dangers of allowing tech companies to do so are similar.[151]

Facebook, it is worth noting, has long taken a far more active approach than Twitter towards regulating content, in line with its "Community Standards".[152] Reddit has struggled with this issue for years. In 2012, a series of articles on the website Gawker drew attention to large forums (or "subreddits") devoted to sexualising underage girls. These were initially defended by the website on freedom of expression grounds, but later banned as attention snowballed into the mainstream media. In 2015, Reddit introduced a policy whereby particularly offensive subreddits would be quarantined, so that they would only be visible to users who explicitly opted in.[153] This represents a sort of half-way house where content is not entirely blocked but its dissemination is limited.

It is easy to see why this issue has become such a minefield for private sector intermediaries. Supporters of Ms. Criado-Perez contrasted Twitter's swift and energetic response to distribution of the Foley video with its refusal to take action against users who harassed and abused her.[154] Reddit's users compared the decision to prohibit sexualised images of minors with the website's continued hosting of a subreddit devoted to pictures of dead children.[155] Inevitably, when a list of quarantined subreddits was published, users found a vast volume of highly offensive content which had escaped the restrictions.[156] Even Apple, primarily a hardware maker, faced criticism over policies on what content it allows to be sold through its App Store. The company banned an app which tracked the number of deaths caused by drone strikes in Pakistan, Yemen and Somalia in real-time, claiming that it contained "excessively crude or objectionable content".[157]

---

[151] Glenn Greenwald, "Should Twitter, Facebook and Google Executives be the Arbiters of What We See and Read?", Intercept, 21 August 2014. Available at: firstlook.org/theintercept/2014/08/21/twitter-facebook-executives-arbiters-see-read.
[152] Available at: www.facebook.com/communitystandards.
[153] "Content Policy Update", Reddit, 5 August 2015. Available at: www.reddit.com/r/announcements/comments/3fx2au/content_policy_update/?limit=500.
[154] James Ball, "Twitter: from free speech champion to selective censor?" The Guardian, 21 August 2014. Available at: www.theguardian.com/technology/2014/aug/21/twitter-free-speech-champion-selective-censor?CMP=twt_gu.
[155] "Why is it that r/jailbait was shut down, but not r/picsofdeadkids?", Reddit, 7 September 2012. Available at: www.reddit.com/r/AskReddit/comments/zhd5d/why_is_it_that_rjailbait_was_shut_down_but_not/.
[156] "Content Policy Update", Reddit, 5 August 2015. Available at: www.reddit.com/r/announcements/comments/3fx2au/content_policy_update/cttd2li.
[157] Stuart Dredge, "Apple removed drone-strike apps from App Store due to 'objectionable content'", The Guardian, 30 September 2015. Available at: www.theguardian.com/technology/2015/sep/30/apple-removing-drone-strikes-app.

Illegal Content

Although private sector intermediaries have considerable flexibility in terms of the material they classify as offensive or against the standards of their services, they have little control over what material is prohibited by law. However, there are significant differences in how private sector intermediaries decide to deal with content which is illegal or of questionable legality. Among the most important factors in determining this is whether, and under what circumstances, intermediaries are protected against liability for the content in relation to which they provide services. Many legal systems grant intermediaries some degree of immunity, although this can come with various conditions. For example, in the United States, private sector intermediaries are protected by section 230 of the Communications Decency Act[158] and section 512 of the Digital Millennium Copyright Act (DMCA).[159] However, the DMCA protections against liability for copyright infringement depend on private sector intermediaries' compliance with "notice and takedown" procedures designed to promote the expedited removal of infringing material.

Although legal rules on immunity from liability are a significant factor in guiding their behaviour, many intermediaries commit to or take actions which go significantly beyond the minimum requirements. This is particularly true in relation to combating the spread of child sexual abuse imagery, which is of course a particularly heinous social ill.

For example, the GNI Implementation Guidelines,

> Acknowledge and recognize the importance of initiatives that seek to identify, prevent and limit access to illegal online activity such as child exploitation. The Principles and Implementation Guidelines do not seek to alter participants' involvement in such initiatives.[160]

Although the Guidelines broadly support measures to combat illegal activity, the specific reference to child exploitation should be seen in light of the fact that many intermediaries have demonstrated a willingness to take more intrusive action in this area. This is likely due to the fact that child sexual abuse is vastly more harmful than, say, copyright infringement, and because contextual considerations like fair use or fair dealing are far less relevant, making it easier to identify illegal content definitively.

Several major tech firms maintain databases of identifying markers (hashes) which automatically identify child sexual abuse imagery. This includes Microsoft's

[158] 47 U.S.C. § 230. Available at: www.law.cornell.edu/uscode/text/47/230.
[159] 17 U.S. Code § 512. Available at: www.law.cornell.edu/uscode/text/17/512.
[160] Available at: globalnetworkinitiative.org/implementationguidelines/index.php.

PhotoDNA technology, which has been in use since 2009.[161] The same system has been used by Facebook since 2011.[162] In 2014, a similar programme run by Google came to light after a tip off from the company to the authorities led to a conviction for child pornography in the United States.[163] Although this particular activity by Google attracted little controversy, some commentators expressed unease at the possibility that a similar approach might be used in other areas of law enforcement, leading to searches for broader incriminating phrases, such as "assassinate the president".[164]

Some intermediaries also go beyond minimum legal requirements to combat hate speech. In particular, intermediaries often face significant pressure from governments to take a more proactive stance in situations where there is a risk of hate-sponsored violence. In Germany, in the wake of xenophobic attacks on refugee camps, the Justice Minister called on Facebook to do more to reign in abusive posts. In response, the company promised to work with the government to create a task force aimed at flagging and removing hateful content more quickly and to help finance organisations which track online speech.[165]

Copyright

By far the most pervasive illegal content issue online is the use of the Internet to violate copyright rules. By making it vastly easier to copy, manipulate and share information, the digital age has led to an explosion in copyright infringement. Some have argued that the mass violation of copyright laws suggests that those laws are poorly adapted to the digital age, and badly in need of reform.[166] But the reaction of many States has been to expand copyright rules rather than to revise them to take digital realities into account.

---

[161] Anthony Salcito, "Microsoft donates PhotoDNA technology to make the Internet safer for kids", Microsoft Developer Blog, 17 December 2009. Available at: blogs.msdn.microsoft.com/microsoftuseducation/2009/12/17/microsoft-donates-photodna-technology-to-make-the-internet-safer-for-kids/.

[162] Catharine Smith, "Facebook Adopts Microsoft PhotoDNA To Remove Child Pornography", Huffington Post, 20 July 2011. Available at: www.huffingtonpost.com/2011/05/20/facebook-photodna-microsoft-child-pornography_n_864695.html.

[163] James Vincent, "Google scans Gmail accounts for child abuse - and has already helped convict a man in the US", The Independent, 4 August 2014. Available at: www.independent.co.uk/life-style/gadgets-and-tech/google-tips-off-us-police-to-man-storing-images-of-child-abuse-on-his-gmail-account-9647551.html.

[164] Jonathan Zittrain, "A Few Keystrokes Could Solve the Crime. Would You Press Enter?", Just Security, 12 January 2016. Available at: www.justsecurity.org/28752/keystrokes-solve-crime-press-enter/.

[165] Amar Toor, "Facebook will work with Germany to combat anti-refugee hate speech", The Verge, 15 September 2015. Available at: www.theverge.com/2015/9/15/9329119/facebook-germany-hate-speech-xenophobia-migrant-refugee.

[166] Centre for Law and Democracy, "Reconceptualising Copyright: Adapting the Rules to Respect Freedom of Expression in the Digital Age", (Halifax: Centre for Law and Democracy, 2013). Available at: www.law-democracy.org/live/wp-content/uploads/2013/07/Final-Copyright-Paper.pdf.

The pervasiveness of copyright infringement has led to the establishment of robust systems for identifying and removing infringing content. Despite this, there is little evidence that these systems have made a dent in the illegal spread of copyrighted material and infringement remains as ubiquitous as ever. At the same time, the systems put in place to address copyright have proven susceptible to abuse.

When Ashley Madison, a website that facilitates adultery, was hacked in 2015, resulting in the publication of sensitive user information, the company responded by sending out a barrage of copyright notifications under the DMCA to try to remove the material.[167] Although the Ashley Madison hack represented a serious invasion of the privacy of millions of individuals, this is unrelated to the purpose of the DMCA and the takedown requests were frivolous and clearly abusive. For example, targets which were successfully taken down included a website which allowed individuals to check whether their private information had been compromised, a critically important service in the aftermath of a major data breach.

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

Across Latin America, there are many examples of abusive uses of the DMCA system, particularly for political purposes. In Ecuador, President Rafael Correa has become notorious for this behaviour:

- On 9 October 2013, Ecuadorian filmmaker Pocho Alvarez discovered that one of his documentaries had been removed from his YouTube page due to alleged copyright infringement. The documentary in question, Assault on Intag, is a short exposition on the harassment suffered by the indigenous community for its resistance to mining activities in the region. It included less than 20 seconds of images of Ecuador's President Correa, including a short clip of his voice. The removal was based on a claim that Alvarez had violated copyright rules by using footage of President Correa taken from his weekly national broadcast. It is interesting to note that Correa filed the claim through a Spanish agency in the United States, rather than in his own country. Another documentary, by filmmaker James Villa, which criticised the Correa administration was also removed due to having used images from his weekly public address. These clearly fall into the scope of exceptions to copyright protection.
- In September 2014, a video depicting the violent repression of a student demonstration, which included apparent police abuses as well as depictions of President Correa praising the police's actions, was removed from Facebook and YouTube after a copyright complaint.
- A Twitter account belonging to Diana Amores was subject to several removal requests after she posted images of politicians with humorous taglines. The

[167] Adam Clark Estes, "Ashley Madison Is Sending Out Bogus DMCA Takedown Notices", Gizmodo, 20 August 2015. Available at: gizmodo.com/ashley-madison-is-sending-bogus-dmca-takedown-notices-1725372969.

volume of complaints led to her account being suspended on multiple occasions. The complaints originated from from EcuadorTV, the State-run TV station, and Movimiento Alianza País, the country's governing party.

Political abuse of the DMCA system is not limited to Ecuador:

- The Ministerial Church of Jesus Christ International, associated with the Colombian political party MIRA, has repeatedly sought the removal of YouTube videos that feature, for example, declarations made by the church's founder. One of the videos that YouTube blocked upon the church's request informed the viewer explicitly – in its title – that the video was a parody.
- In Brazil, the DMCA was used to remove critical videos of 2014 presidential candidate and former governor, Aécio Neves. Although the requester's identity has not been confirmed, many speculated that Neves himself was responsible for the takedowns.

The public interest is affected each time legitimate content is removed from the Internet. The public interest is engaged if the content removed can be legally sent or received according to intellectual property laws (such as content in the public domain, "fair use" or other copyright exceptions). In many cases, content is removed based on an incorrect balancing between copyright and freedom of expression. This is a serious imbalance because freedom of expression is a fundamental human right, while copyright is not.

In 2015, a hacker leaked an enormous trove of internal information from Hacking Team, a spyware and surveillance company, onto the Internet.[168] The leak included evidence that the company had sold their equipment to Sudan, potentially in breach of UN sanctions, as well as to intelligence agencies in Egypt, Ethiopia, Kazakhstan, Russia and Saudi Arabia, all States which are known to persecute journalists and opposition figures. The company's immediate response was to send out frivolous DMCA notifications in an attempt to stop the spread of the leaks.

The DMCA system was even used by the United States' National Association for Stock Car Racing (NASCAR) to try and remove footage of a major car crash at one of their events.[169] NASCAR defended its actions as a matter of respecting the privacy of those injured, again not the problem the DMCA was designed to address. From a human rights perspective, measures which can easily be expanded beyond their intended purpose, like the DMCA, are troubling since they are by definition overbroad, running counter to the cardinal principle, as spelled out in the

[168] Cory Doctorow, "Hacking Team leak: bogus copyright takedowns and mass DEA surveillance in Colombia", BoingBoing, 7 July 2015. Available at: boingboing.net/2015/07/07/hacking-team-leak-bogus-copyr.html.
[169] Mike Masnick, "NASCAR Abuses DMCA To Try To Delete Fan Videos Of Daytona Crash", Techdirt, 25 February 2013. Available at: www.techdirt.com/articles/20130224/22411222089/nascar-abuses-dmca-to-try-to-delete-fan-videos-daytona-crash.shtml.

International Covenant on Civil and Political Rights (ICCPR),[170] that laws which restrict expression should be carefully and narrowly construed.

Furthermore, many private intermediaries go beyond what is legally required when dealing with potentially infringing content. The starkest example of this is in South Korea, where legal ambiguities and an eagerness to avoid liability have led to intermediaries complying with virtually every request they receive, resulting in a rate of removal that far exceeds that of other comparable countries.

Open Net Korea

The Korea Communications Standards Commission (KCSC), the administrative body responsible for monitoring and restricting Internet content in Korea, generally attempts to remove information through the use of "non-binding" requests rather than formal takedown decisions. This avoids having to provide subjects with notice and a hearing or any other procedural safeguards. Although private sector intermediaries can refuse to comply with these requests, the compliance rate is effectively 100 percent, partly because South Korea has extremely weak protections against intermediary liability, incentivising intermediaries to comply with requests without questioning them.

No intermediary has ever challenged a KCSC decision in court. Although users can file objections, they rarely do since the intermediary, rather than the user, is notified of the takedown request. This is particularly problematic in light of the fact that in some cases the users, properly notified, would likely volunteer to remove just the offending material. Instead, takedowns are often vastly overbroad. For instance, an entire blog maintained by a 60-year-old man was shut down following a KCSC request because about one-third of 132 entries included content deemed to be supportive of North Korea, which is illegal under the National Security Act (which is a highly problematic document on its own). About half of the entries were photos of his grandchildren, pictures of his own paintings, music and singing files of his own composition, and cooking recipes, accumulated over 3-4 years late in the man's life. Had he been notified, it is likely that he would have deleted the pro-North Korean statements in order to protect his other, legal content, or at least have backed-up the other content to prevent it from being lost.

Overall, South Korea's system of content removal is extremely pervasive. In 2013, the KCSC ordered the blocking or deletion of 104,400 websites. By comparison, their counterpart in Australia, the Australian Communication and Media Authority (ACMA), only blocked about 500 websites in 2013.

The KCSC's takedowns often target frivolous sites, or sites that criticise politicians.

[170] UN General Assembly Resolution 2200A(XXI), adopted 16 December 1966, in force 23 March 1976.

Government officials often make private takedown requests for postings that criticise their policy decisions. Some examples of this include:

- A posting criticising a Seoul City mayor's ban on assemblies in Seoul Square;
- A posting criticising a legislator's drinking habits and publicising his social media account;
- Clips of a television news report on the Seoul Police Chief's brother who allegedly runs an illegal brothel;
- A posting criticising politicians' pejorative remarks about the recent deaths of squatters and police officers in a redevelopment dispute;
- A posting calling for immunity for labour strikers from criminal prosecutions and civil damage suits;
- A posting by an opposition party legislator questioning a conservative media executive's involvement in a sex exploitation scandal related to an actress and her suicide; and
- A Twitter account titled 2MB18NOMA was blocked because the phonetic name of the account resembles an epithet against the then-President Lee Myung-Bak.

Although the DMCA offers private online intermediaries greater protection from liability that they have under South Korean law, it nonetheless heavily incentivises over-compliance, since protection is predicated upon their promptly removing content upon receiving notice from the rights holder. Consequently, some intermediaries have been criticised for failing to stand up for their users in the face of frivolous DMCA takedown requests, or their failure to investigate whether a complaint is meritorious, or engage with users after a complaint has been filed.

YouTube's ContentID system, which is another voluntary mechanism, automates the process of flagging and removing allegedly infringing content.[171] This can lead to mistakes. For example, the system has repeatedly flagged footage posted by the National Aeronautics and Space Administration (NASA), despite the fact that, like all United States government agencies, its content is in the public domain.[172] There have also been reports of users having original material which they created flagged.[173] In addition to these mistakes, the automation of the system means that it is unable to take into account possible defences to copyright infringement, such as fair use.

---

[171] A brief explanation of how the system works is available at: www.youtube.com/watch?v=9g2U12SsRns#t=33.

[172] Mike Masnick, "Curiosity's Mars Landing Video Disappears From YouTube Due To Bogus Copyright Claim", Techdirt, 6 August 2012. Available at: www.techdirt.com/articles/20120806/11053019945/curiositys-mars-landing-video-disappears-youtube-due-to-bogus-copyright-claim.shtml.

[173] Erik Kain, "YouTube Responds To Content ID Crackdown, Plot Thickens", Forbes, 17 December 2013. Available at: www.forbes.com/sites/erikkain/2013/12/17/youtube-responds-to-content-id-crackdown-plot-thickens/#339f50001086.

Centre for Internet and Society

ISPs in India often respond to takedown requests by removing far more material than is required. One solution to this is for courts to be more specific in their orders, but ISPs also need to take a stronger stand in favour of freedom of expression and interpret these orders as narrowly as possible.

Only one of the companies we examined, SingTel, provided their users with notice when material had been removed on copyright grounds. None of the companies we examined provided a specific redress mechanism to individuals whose material was wrongfully removed.

Internet access providers in the United States have also agreed to participate in voluntary schemes aimed at combating copyright infringement, most notably the Copyright Alert System (CAS), otherwise known as "Six Strikes".[174] This system, which was launched in February 2013, allows for escalating responses to instances of copyright infringement beginning with "educational" alerts and escalating to more intrusive measures, including penalties. The specific enforcement measures vary among access providers, and there is a lack of consistency, or transparency, as to how users may be impacted. For example, Verizon has stated that, on the fifth alert, users' Internet access speed will be throttled to 256kbps for a period of two days.[175] Optimum Online, another Internet access provider, states that upon receiving an alert it "may temporarily suspend your Internet access for a set period of time, or until you contact Optimum."[176] It is worth noting that a 2011 Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression states:

> The Special Rapporteur considers cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights.
>
> The Special Rapporteur calls upon all States to ensure that Internet access is maintained at all times, including during times of political unrest. In particular, the Special Rapporteur urges States to repeal or amend existing intellectual copyright laws which permit users to be disconnected from Internet access, and to refrain from adopting such laws.[177]

---

[174] Center for Copyright Information, "The Copyright Alert System". Available at: www.copyrightinformation.org/the-copyright-alert-system/.
[175] Verizon, "Copyrights and Verizon's Copyright Alert Program". Available at: www.verizon.com/support/consumer/account-and-billing/copyright-alert-program-faqs#04FAQ.
[176] Optimum, "Copyright Infringement Alerts". Available at: optimum.custhelp.com/app/answers/detail/a_id/3592.
[177] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27, paras. 78 and 79. Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

Widespread misuse of the system suggests that, before any claimant completes the form to report an alleged infringement, they should be presented with instructions explaining:

a. The conditions under which a copyright claim will be legitimate.
b. The difference between being a copyright holder and the right to ones image.
c. What constitutes abuse of the DMCA, as well as the possible sanctions for this abuse. Private sector intermediaries should make it clear that users who repeatedly file abusive complaints may also be subject to penalties, such as the cancellation of their accounts.
d. A list of exceptions to copyright, as explained according to local legal standards.

Stand Up For Digital Rights

Recommendations for Moderation and Removal of Content:

Clarity and Communication

- **Intermediaries should post, in a prominent place, clear, thorough and easy to understand guides to their policies and practices for taking action in relation to content, including detailed information about how they are enforced. Where policies need to be complex due to the fact that they form the basis of a legal contract with users, they should be accompanied by clear, concise and easy to understand summaries or explanatory guides.**
- **Intermediaries' copyright reporting mechanisms should provide information to both complainants and users about limitations and exceptions to copyright and, where applicable, warn complainants about the potential consequences of filing false claims.**
- **Policies to address problematic content (such as deletion or moderation) which go beyond formal legal requirements should be based on clear, pre-determined policies which can be justified by reference to a standard which is based on objective criteria (such as a family friendly service) which are set out in the policy, and which is not based on ideological or political goals. Where possible, intermediaries should consult with their users when determining such policies.**

Process for Receiving and Adjudicating Complaints

- **Third parties who file a complaint about inappropriate or illegal content should be required to indicate what legal or policy rule the content allegedly violates.**
- **Intermediaries should be consistent in applying any content moderation policies or legal rules and should scrutinise claims under such policies or rules carefully before applying any measures. They should have in place processes to track abuses of their content moderation systems and should apply more careful scrutiny to claims from users who repeatedly file frivolous or abusive claims.**

- **Intermediaries should, subject only to legal or technical constraints, notify users promptly when content which the latter created, uploaded or hosts is subject to a complaint or restriction. The notification should include a reference to the legal or policy rule in question, and an explanation of the procedure being applied, the opportunities available to the user to provide input before a decision is taken, and common defences to the application of the procedure.**
- **Where action is proposed to be taken in relation to content a user has created, uploaded or hosts, that user should normally be given an opportunity to contest that action. Where possible, subject to reasonable resource and technical constraints, users should be given a right to appeal against any decision to take action against the content at issue.**

Restricting Content

- **Actions to remove or otherwise restrict third party content should be as targeted as possible and should only apply to the specific content which offends against the relevant legal or policy standard.**
- **Intermediaries should consider whether less intrusive measures are available which provide protection against harmful content without necessarily taking that content down, such as providing for opt-ins to access the content.**
- **Where action is taken against content, the intermediary should, subject to reasonable technical constraints, retain the means to reverse that action for as long as any appeal against the action, including any legal appeal, remains pending.**
- **Where a user's account is deleted or de-activated, users should be given an option to preserve and export the data from that account, unless the material is patently illegal (i.e. in the case of child sexual abuse imagery) or has been declared to be illegal by a clear and binding legal order.**

Key Issues: Addressing Privacy Concerns Online

The right to privacy is internationally recognised as a human right, protected in Article 12 of the *Universal Declaration of Human Rights*:[178]

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The right to privacy is also guaranteed by the ICCPR, the *American Convention on Human Rights*[179] and the *European Convention on Human Rights,*[180] as well as in most national constitutions.

In addition to its importance in its own right, privacy is linked to the fulfilment of the right to freedom of expression. Studies have shown that perceptions of control over one's communications, including over who has access to them, lead to franker and more extensive communications, while a loss of control leaves people feeling less free to engage earnestly.[181] The nexus between privacy and freedom of expression has been noted by the UN Special Rapporteur on Freedom of Opinion and Expression:

> States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy… Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.[182]

Privacy has been particularly affected by digital developments to the point where the Internet has had a dramatic impact on our understandings of the very concept of privacy. On the one hand, the Internet provides for an unprecedented level of freedom and anonymity, where tastes can be explored or opinions expressed without regard to what one's family, friends or social circle might think. For a gay Ugandan or Russian, or a Saudi atheist, the Internet may provide the only avenue for self-expression or to network with likeminded communities.

---

[178] UN General Assembly Resolution 217A(III), 10 December 1948.
[179] Adopted 22 November 1969, O.A.S. Treaty Series No. 36, entered into force 18 July 1978.
[180] Adopted 4 November 1950, E.T.S. No. 5, entered into force 3 September 1953.
[181] Tamara Dinev, Heng Xu, Jeff H. Smith and Paul Hart, "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts" 22 European Journal of Information Systems (2013), p. 300. Available at: www.palgrave-journals.com/ejis/journal/v22/n3/pdf/ejis201223a.pdf.
[182] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/23/40, 17 April 2013, para. 79.

On the other hand, the Internet is also the most heavily monitored and tracked medium of expression in history, where every move that users make is noted, followed and recorded. Reading a newspaper article, going out on a date or attending an event in the real world are transient events. For the most part, evidence of one's activity disappears after the fact. Online, however, a person's activities, even mundane ones, leave footprints which can be traced by commercial and government actors who are interested in studying, processing and collating this information for various reasons. The permanence of digital records compounds this, since actions taken years ago remain traceable. A poorly thought out blog comment or an erroneous news story can end up as the top result of a web search for a person's name even years after the event.

Commercial Models and Privacy

While the privacy issues noted above are troubling, the fact is that the sale of personal information, and the use of targeted advertising which is facilitated by the collection of personal information, are major economic forces behind the spread of Internet services, since they are the core business model which allows many tech companies to offer their products and services free of direct charges on users. Despite the success of this model, it has been referred to as the Internet's "original sin" and some people have urged private sector intermediaries to explore alternative business models which allow for sustainable growth without compromising user privacy.[183] In response to such demands, Google already offers a subscription version of its email service for businesses which is ad-free.[184]

Ultimately, of course, it remains the prerogative of companies as to whether they wish to pursue alternative business models subject, of course, to compliance with the law. However, even if one embraces the idea that exchanging privacy for free services online is a fair trade, ground rules are needed. The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in a 2011 report that States have a responsibility to protect consumers:

> States parties are required by article 17(2) [of the ICCPR] to regulate, through clearly articulated laws, the recording, processing, use and conveyance of automated personal data and to protect those affected against misuse by State organs as well as private parties.[185]

---

[183] Ethan Zuckerman, "The Internet's Original Sin", The Atlantic, 14 August 2014. Available at: www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/.

[184] Available at: www.google.com/work/apps/business/.

[185] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27, 16 May 2011, para. 58. Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

A similar sentiment was expressed in the UN Human Rights Committee's General Comment on the right to privacy:

> 10. The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.[186]

It is arguable that the intrusiveness of State regulation over companies in this area should depend, at least in part, on the extent to which industry acts to offer effective protections of its own.

A key issue here is being clear and transparent with users about policies around collecting, sharing and processing information, so that they understand them and adapt their expectations and business patronage accordingly. For example, while users may implicitly understand that their private information is being processed by companies whose business model is based on advertising, such as Google and Facebook, revelations of data collection schemes by Apple, whose primary business is selling hardware, surprised consumers.[187] Intrusive behaviour from companies which explicitly market the privacy features of their services, such as the app Whisper, are particularly egregious.[188]

Similarly, users may implicitly understand that information will be used to track their actions in an automated or aggregated way, and for advertising purposes, but not expect it to be examined by human beings. In 2014, a tech blogger received leaked internal information via a Microsoft Hotmail account relating to the upcoming release of Windows 8.[189] When the blogger attempted to confirm the veracity of the material with Microsoft, the company went through the blogger's Hotmail account to identify the source of the leak. Microsoft defended its behaviour by citing its terms of service, which included a line allowing access to users' accounts to protect the company's rights or property. However, commentators noted that the language of the policy was broad enough to allow access to virtually any account, for virtually any reason, and that the actions meant that Microsoft's broad claims about privacy protection were misleading. As a consequence of the backlash, Microsoft eventually refined its terms of service so that they would, in

---

[186] Human Rights Committee, General Comment 16, U.N. Doc. HRI/GEN/1/Rev.1, p. 21 (1994). Available at: www1.umn.edu/humanrts/gencomm/hrcom16.htm.
[187] Andy Greenberg, "How to Stop Apple From Snooping on Your OS X Yosemite Searches", Wired, 20 October 2014. Available at: www.wired.com/2014/10/how-to-fix-os-x-yosemite-search/.
[188] Paul Lewis and Dominic Rushe, "Revealed: how Whisper app tracks 'anonymous' users", The Guardian, 16 October 2014. Available at: www.theguardian.com/world/2014/oct/16/-sp-revealed-whisper-app-tracking-users.
[189] Andrew Crocker, "Microsoft Says: Come Back with a Warrant, Unless You're Microsoft", Electronic Frontier Foundation, 21 March 2014. Available at: www.eff.org/deeplinks/2014/03/microsoft-says-come-back-warrant-unless-youre-microsoft.

future, leave such cases to the law enforcement authorities rather than undertaking their own investigations.[190]

More generally, the increasing involvement of third party data brokers in collecting and processing users' information raises concerns due to the opacity of the process and the lack of any direct relationship between the users and the data brokers. The fact that most users have no idea what companies or even types of companies their data will be shared with, or even any idea what kind of uses it will be put towards, mean that it is hard to accept that their agreement meets the standard of "informed consent". Research carried out in May 2014 showed that 88 percent of the 950,489 most popular websites on the Internet sent user information to third-parties.[191] Of the sites which shared information with third parties, an average of 9.47 different web domains were contacted per user visit. The vast majority of this tracking was carried out surreptitiously, with only two percent of the third parties including a visible prompt alerting users to their presence.

Third-party advertising is a legitimate and even vital part of the Internet's economic ecosystem. However, the lack of clarity surrounding the practice and the impossibility for users to know who is doing what with their personal information raises serious privacy concerns. This is particularly true given that privacy invasions can become far more intrusive when personal information is collated from multiple sources. As an example, a mobile app called Girls Around Me draws information from social media, including photos, interests and the like, and combines it with data from Foursquare, a geo-location mobile app, to allow users to browse realtime information about women in their vicinity. The combination created a programme which was highly intrusive and which observers dubbed a "let's stalk women" app.[192] Girls Around Me raises additional concerns about physical and sexual violence, but it is easy to see how combining datasets from various sources, as some apps do, can create a far more privacy invading picture of an individual.

A concrete manifestation of users' frustration with intrusive online tracking and advertising is the rise in popularity of ad blocking software. The most popular tool for this, AdBlock, has seen a steep rise in its user base since 2013.[193] The service was projected to exceed 236 million users by the end of 2015, with a particular concentration in Europe. This represents a serious challenge for private sector

[190] Andrew Crocker, "Reforming Terms of Service: Microsoft Changes Its Policy on Access to User Data", Electronic Frontier Foundation, 28 March 2014. Available at: www.eff.org/deeplinks/2014/03/reforming-terms-service-microsoft-changes-its-policy-access-user-data.

[191] Timothy Libert, "Exposing the Hidden Web: Third-Party HTTP Requests on One Million Websites, International Journal of Communication, October 2015. Available at: ijoc.org/index.php/ijoc/article/download/3646/1503.

[192] Nick Bilton, "Girls Around Me: An App Takes Creepy to a New Level", The New York Times, 30 March 2012. Available at: bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/?_r=0.

[193] Ricardo Bilton, "The global rise of ad blocking in 4 charts", Digiday, 1 June 2015. Available at: digiday.com/publishers/global-rise-ad-blocking-4-charts/.

intermediaries whose business model is based on advertising. From their perspective, it does not seem fair for users to enjoy their services while opting out of the system which pays for it. Even if alternative revenue models are encouraged, there is a strong collective interest in maintaining the viability of ad-supported services, to ensure that useful websites remain accessible to everyone.

Some have drawn a connection between the rise in ad blocking and a decision by major private sector intermediaries not to respect "do not track" (DNT) messages from users.[194] DNT is a mechanism which allows users to indicate to websites they visit that they do not wish to be tracked. However, DNT is only effective if private sector intermediaries choose to respect the request. Several major players, including Google, Facebook and Yahoo!, have indicated publicly that they will not respect DNT requests.[195] Given the ability of AdBlock users to "whitelist" particular websites, and indications that their user base would be happy for them to do this for sites which respect user privacy and are not overly intrusive in their advertising methods, the spread of blocking software creates a growing incentive for the industry to develop better standards regarding advertising and user tracking.

Anonymity

Anonymisation tools can be very important to protecting online privacy, particularly in sensitive contexts. A 2011 report of the UN Special Rapporteur on freedom of expression noted that State limitations on the ability of users to communicate anonymously represented a restriction on freedom of expression which needed to be assessed using the three-part test for such restrictions:

> [The Special Rapporteur] also calls upon States to ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems. Under certain exceptional situations where States may limit the right to privacy for the purposes of administration of criminal justice or prevention of crime, the Special Rapporteur underscores that such measures must be in compliance with the international human rights framework, with adequate safeguards against abuse. This includes ensuring that any measure to limit the right to privacy is taken on the basis of a specific decision by a State authority expressly empowered by law to do so, and must respect the principles of necessity and proportionality.[196]

---

[194] See Doc. Searls Weblog, "Beyond ad blocking - the biggest boycott in human history", 20 September 2015. Available at: blogs.law.harvard.edu/doc/2015/09/28/beyond-ad-blocking-the-biggest-boycott-in-human-history/.

[195] Jim Edwards, "In A Further Humiliation To Microsoft, Facebook Will Not Honor 'Do Not Track' Signals On Internet Explorer ", *Business Insider*, 12 June 2014. Available at: www.businessinsider.com/facebook-will-not-honor-do-not-track-2014-6.

[196] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, note 177, paragraph 84.

The Council of Europe's *Declaration on Freedom of Communication* also calls on States to respect Internet users' wish not to be identified:

> In order to ensure protection against online surveillance and to enhance the free expression of information and ideas (…) States should respect the will of users of the Internet not to disclose their identity.[197]

Arabic Network for Human Rights Information

The majority of the Internet experts surveyed during the course of our research did not trust the ability of private sector intermediaries to protect their personal data, due to the absence of clear rules for the protection of personal data. The pervasive regime of surveillance in Egypt and the lack of laws and policies protecting Internet privacy led many users and online activists to rely on Tor, and other applications providing encryption or anonymity.

Unfortunately, despite the presence of a large number of companies that provide telecommunications and Internet services in the Arab region, we did not observe substantial differences between those companies in relation to the protection of the personal data of users.

As discussed earlier, the facelessness of online discussions facilitates the ability of users to express themselves without fear of social repercussions. As Oscar Wilde once said, "Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth."[198] Among many online communities, there is a strong taboo against "doxxing", publishing personally identifiable information about a person, particularly when they are using an online alias.[199]

The Internet has become an important means for communicating information about sensitive subjects, such as sexual or mental health issues and child abuse. The Internet has also become the key means for whistleblowers seeking to expose corruption or other wrongdoing. Although, for security reasons, Edward Snowden's main disclosures were delivered physically via USB sticks, he made contact with the journalists and set up the handoff through the Internet. Websites like Wikileaks could not exist without the promises of anonymity which they provide. Although some of their reporting has been controversial, they provide an important public interest service. For example, the negotiations over the Trans-Pacific Partnership, a

---

[197] Council of Europe, Declaration on Freedom of Communication on the Internet, 2003, Principle 7. Available at: coe.int/t/informationsociety/documents/Freedom%20of%20communication%20on%20the%20Internet_en.pdf.

[198] See: www.goodreads.com/quotes/3736-man-is-least-himself-when-he-talks-in-his-own.

[199] See: "What doxxing is, and why it matters", The Economist, 10 March 2014. Available at: www.economist.com/blogs/economist-explains/2014/03/economist-explains-9.

sweeping trade deal involving twelve countries, were conducted in almost total secrecy, with civil society groups being excluded. Unauthorised releases of the draft text on Wikileaks provided these groups with the information they need to monitor the process.[200]

The centrality of the Internet to sensitive communications, and the level of trust that its users have in its capacity to protect their identities, when they are asking for that, means that failures on this front can have particularly stark consequences. In 2014, a researcher discovered a security glitch in "Grindr", a popular smartphone app targeting gay men, through which the location of any of its users could be identified to within a 30-metre margin of error. By exploiting this glitch, users were able to locate 189 users of the app in Iran, where homosexuality is illegal.[201]

Christopher Parsons

Companies can influence potential State surveillance capabilities based on how the companies collect and analyse telecommunications traffic data for their own business purposes. In the United States, AT&T engineers built a system in the late 1990s to data mine the company's telephone and Internet access records. It was "originally created to develop marketing leads and as an anti-fraud tool to target new customers who called the same numbers as previously identified fraudsters" but in 2007 "it was revealed that the FBI had been seeking 'community of interest' or 'calling circle' records from several telecommunications providers." [202] AT&T was able to comply with these requests because of the data mining system it had built for legitimate business purposes. One of its competitors, Verizon, was unable to perform equivalent surveillance for the FBI because it did not have a comparable data mining system.[203]

In a related vein, the period of time for which private sector intermediaries retain data can affect the availability of information to government agents. In the Canadian context, one of the country's largest home Internet providers, Rogers, must retain records of the Uniform Resource Locators (URLs) that subscribers visit for at least

[200] Centre for Law and Democracy, Analysis of the Draft Intellectual Property Chapter of the TransPacific Partnership, December 2013. Available at: www.law-democracy.org/live/wp-content/uploads/2013/12/TPP.IP-final.Dec13.pdf.

[201] John Aravosis, "Grindr smartphone app outs exact location of gays across Iran", America Blog, 27 August 2014. Available at: americablog.com/2014/08/grindr-smartphone-app-outs-exact-location-gays-across-iran.html.

[202] Christopher Soghoian, "The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance," Doctoral Dissertation, July 2012, pp. 29. Available at: files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf. Accessed 17 November 2015.

[203] *Ibid.* It must be noted, however, that the absence of the system did not prevent the US government from accessing or analysing communications records. Instead, Verizon and other telephone companies provided the National Security Agency (NSA) with access to call records and the NSA itself performed the community of interest analysis.

31 days; these records are needed in order to notify customers when they approach their allocated monthly bandwidth limits.[204] One of Rogers' competitors, Teksavvy, maintains a 0-day retention protocol. One consequence of these different business models is that government authorities could request Rogers to divulge a particular subscriber's web history and expect it to be provided retroactively. To get URL records from Teksavvy, however, the same authorities would need to compel Teksavvy to start keeping logs about a particular subscriber's communications activities, and these could only be available on a proactive basis. On the other hand, Rogers can retroactively provide details of its subscribers' call records going back as far as ten years whereas TekSavvy retains similar records indefinitely.

There are legitimate reasons why some private sector intermediaries may want to require real-name registration. For example, Airbnb, a website which allows users to rent lodging from one another, has been moving towards verifying their users as a security measure. This is fair enough, as a step to enhance trust between renters and hosts, who both have understandable safety concerns. It is worth noting that Airbnb also insures renters against property damage caused by guests, giving the website a direct reason for seeking information about its users. LinkedIn, a professional networking site, also requires real names. This too, seems fairly core to their business model, which relies on users believing that the CV they are browsing is reasonably accurate. Other services claim that requiring real-name registration improves the civility of the online discourse. Whether or not this is true in practice is open to debate, but it is a legitimate model to pursue. In an effort to improve the quality and tone of comments on YouTube, Google, which owns the video-sharing site, imposed a real-name requirement in 2013, but this was unpopular and Google reversed the move after less than a year.[205]

However, while online intermediaries have a legitimate interest in exercising discretion as to whether or not to require real-name registration, these decisions should also take into account the broader human rights implications, and the degree of impact that the requirement has on their users. For a site like Airbnb, the freedom of expression impact of requiring real names is minimal. For a site like Facebook, on the other hand, their dominant market position, and the fact that so many people use it as a primary communications platform, including in many repressive States, alters the calculus. Facebook's real-name requirement has been criticised by some. To the company's credit, in 2015 they announced changes to their policy allowing

[204] Christopher Parsons, "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, 2015, pp. 51. Available at: www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[205] Samuel Gibbs, "The return of the YouTube troll: Google ends its 'real name' commenter policy", The Guardian, 16 July 2014. Available at: www.theguardian.com/technology/2014/jul/16/youtube-trolls-google-real-name-commenter-policy.

for the use of pseudonyms under some circumstances, such as where a user is transgender, a victim of stalking or faces abuse or discrimination.[206]

All intermediaries have a responsibility to be fully transparent with their users as to the extent to which any anonymity they offer or appear to be offering will be respected. The reason why a data breach at Grindr is so serious is because the service is predicated on discretion, which significantly elevates the sensitivity of the information that users will entrust to it. Perceptions, and building realistic expectations, are of cardinal importance here.

As part of this, intermediaries should also make sure that, where they claim to have "anonymised" information before it is shared with third parties, they do so properly. In 2006, AOL Inc. published the Internet search histories of 650,000 of its users as a resource for academic researchers, after undertaking measures to anonymise the data. However, New York Times reporters and others were able to reconnect the data to identifiable individuals because anonymisation had not been done properly.[207] As a consequence, the researcher responsible for releasing the data and AOL's Chief Technology Officer both resigned. While making this sort of information available for research purposes is invaluable, at the same time it is important to anonymise it properly before releasing it.

Security and Encryption

Another means of protecting user privacy is through strong data security measures and the use of encryption. In 2015, the UN Special Rapporteur on freedom of expression specifically noted the importance of encryption to freedom of expression:

> Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity.
> ...
> The use of encryption and anonymity tools and better digital literacy should be encouraged. The Special Rapporteur, recognizing that the value of encryption and anonymity tools depends on their widespread adoption, encourages States, civil society organizations and corporations to engage in a campaign to bring encryption

[206] Todd Gage and Justin Osofsky, "Community Support FYI: Improving the Names Process on Facebook", Facebook Newsroom, 15 December 2015. Available at: newsroom.fb.com/news/2015/12/community-support-fyi-improving-the-names-process-on-facebook.

[207] Castan Centre for Human Rights Law, International Business Leaders Forum, and Office of the United Nations High Commissioner for Human Rights, Human Rights Translated – A Business Reference Guide (2008). Available at: www2.ohchr.org/english/issues/globalization/business/docs/Human_Rights_Translated_web.pdf.

> by design and default to users around the world and, where necessary, to ensure that users at risk be provided the tools to exercise their right to freedom of opinion and expression securely.[208]

While the report mainly targeted States, who have made significant efforts to undermine or prevent the use of encryption in recent years, it also included recommendations for corporate actors:

> Corporate actors should likewise consider their own policies that restrict encryption and anonymity (including through the use of pseudonyms).
> …
> States, international organizations, corporations and civil society groups should promote online security. Given the relevance of new communication technologies in the promotion of human rights and development, all those involved should systematically promote access to encryption and anonymity without discrimination.
> …
> While the present report does not draw conclusions about corporate responsibilities for communication security, it is nonetheless clear that, given the threats to freedom of expression online, corporate actors should review the adequacy of their practices with regard to human right norms… Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication.

Edward Snowden, who is famous for exposing major mass surveillance programmes by Western governments, also pointed to the role that encryption could play in restoring user privacy on the Internet, noting that consumers and corporations held the keys to the effective use of encryption:

> We have the means and we have the technology to end mass surveillance without any legislative action at all, without any policy changes. By basically adopting changes like making encryption a universal standard—where all communications are encrypted by default—we can end mass surveillance not just in the United States but around the world.[209]

In the aftermath of the Snowden revelations, several major players announced moves to encrypt more user information by default.[210] In addition to facilitating and promoting the use of encryption, online intermediaries should consider other means to encourage strong data security among their users, potentially through offering inducements.

Private sector intermediaries should also minimise the amount of data that they hold, including by considering whether maintaining particular information is necessary to accomplish their goals. The more information an organisation

---

[208] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 22 May 2015, para. 56-63.
[209] James Bedford, "The Most Wanted Man in the World", Wired, August 2014. Available at: www.wired.com/2014/08/edward-snowden.
[210] Lorenzo Franceschi-Bicchierai, "Reddit Switches to Encryption By Default", Motherboard, 17 June 2015. Available at: motherboard.vice.com/read/reddit-switches-to-https-encryption-by-default.

maintains, the greater the risk of a security breach.[211] This was a particular lesson from the Ashley Madison hack, since the website maintained information on users who had ceased using their services years ago.[212]

Once security has been breached, it is important for private sector intermediaries to inform those who have or might have been impacted promptly and fully. Where personal information has been compromised, speed can be of the essence in minimising damage. Again, Ashley Madison provides a good example of what not to do. Although the Ashley Madison hackers first announced their intrusion on 15 July 2015, by publishing a small amount of stolen user information, the website initially denied the attack, claiming their system was completely secure and that the hackers had not been successful.[213] Ashley Madison's denials continued until the website's full user information was published the following month.

Right to be Forgotten

Given the Internet's transformative impact on a range of social functions, from work to shopping to socialising, a person's online footprint can be an important aspect of their identity. Employers, colleagues, romantic connections and even casual acquaintances are increasingly likely to look a person up online to find out more about them. While users are able to control the information that they post to websites and social media pages, they have little control over what others post, whether is officials posting information about legal infractions or friends posting pictures. Furthermore, a search for a person's name on a search engine provides information based on the engine's own algorithms. These may promote trivial or negative aspects of a person's background, such as an arrest for underage drinking or a poorly thought out comment. A person's past mistakes can follow them virtually forever on the Internet, becoming an indelible part of their online identity.

There are benefits to making peoples' pasts more accessible. A holocaust museum, for example, has a legitimate interest in knowing if a person they are considering for a job has a history of racist statements, while a women's shelter has a legitimate interest in knowing whether a job applicant has a history of sexism. However, everyone makes mistakes and does things that they do not want to remain fully

[211] Federal Trade Commission, Internet of things: Privacy and Security in a Connected World, January 2015. Available at: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[212] Indeed, this was part of the website's extortionate business model. They charged former users to have their information removed, although the hack demonstrated that even some users who had paid them had not had their information fully deleted. Ashley Madison offered to waive their deletion fee in the aftermath of the hack, in an attempt to close the stable door after the horse had left.
[213] Alex Hern, "Ashley Madison customer service in meltdown as site battles hack fallout", The Guardian, 21 July 2015. Available at: www.theguardian.com/technology/2015/jul/21/ashley-madison-customer-service-meltdown-hack-fallout.

public, forever. From this perspective, the indelibility of digital records raises concerns.

The particular way information is presented can exacerbate the problem. A decision by a prosecutor to drop charges or a trial which fails to result in a conviction may not generate as much media coverage as the initial arrest and may not feature as prominently on a later web search. Similarly, an erroneous and sensational media report may attract more attention than a later retraction. In these cases, a web search may paint a false and unfair picture of the individual.

Steps have been taken in other areas of life to accommodate these concerns. For example, reflecting the idea of giving people second chances, some countries have laws which state that, after a particular period of time, a prior criminal conviction may no longer be taken into account for applicants seeking insurance or employment. Another manifestation of this is the emergent "right to be forgotten", which gives individuals a right to have certain information about themselves removed or blocked from search results.

The right to be forgotten gained particular prominence in 2014, when the European Court of Justice (ECJ) found that Europe's data protection legislation granted EU citizens a right to request that Internet search engines, in that case Google, not display results relating to them which were "inadequate, irrelevant, or no longer relevant, or excessive in relation to the purposes for which they were processed".[214] In processing removal requests, Google is mandated by the ECJ decision to consider whether the overall public interest weighs in favour of continuing to point to the information or not. Assessing this public interest involves a difficult balancing between freedom of expression, the right to information, the right to data protection and the right to privacy. Within three months of the ruling, Google had blocked over 170,000 URLs from being displayed through its searches.[215]

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

The right to freedom of expression, and a person's right to publish content, was completely ignored in the ECJ's analysis of the balance of rights in the Costeja case. Instead, the case was treated as a conflict between the "fundamental rights" of the holder of the data and the "mere economic interest" of the intermediary.

The ECJ held that it was legitimate in certain contexts to request that an Internet

[214] Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:2014:317. Available at: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

[215] David Kravets, "Google has removed 170,000-plus URLs under 'right to be forgotten' edict", Ars Technica, 10 October 2014. Available at: arstechnica.com/tech-policy/2014/10/google-has-removed-170000-plus-urls-under-right-to-be-forgotten-edict/.

intermediary remove or block user-generated content. This raises a question for courts and regulators in Latin America as to whether there may be similar results under the Inter-American Court of Human Rights.

There are many legitimate criticisms of the ECJ's right to be forgotten ruling. For a start, the ruling failed to account properly for freedom of expression and included troubling statements that the interest of the general public in finding information is, as a "general rule", overridden by privacy and data protection rights. This is absolutely not the case under international human rights law. Competing rights must always be balanced against each other. In recognition of this, for example, access to information or right to information laws around the world provide for a balanced weighing of the right to access information and privacy.

A second problem is that search engines, to which the key decision-making responsibilities under this right are delegated, are not well-placed to undertake the delicate balancing between core rights which is required. Determinations about where the larger public interest lies should be made by courts or at the very least publicly constituted decision-makers rather than being foisted onto the private sector. Previous experience with copyright takedowns demonstrates the potential problems with this, as private sector intermediaries have been criticised for failing to consider exceptions to copyright such as fair use or fair dealing properly, given that the easiest and safest choice is to delete anything that might breach the rules. Indeed, in such situations companies can face a conflict of interest or at least tension between their business interests and their broader social and human rights responsibilities.

This problem is compounded by the fact that the ECJ proposed very vague standards for assessing whether material should be removed. Indeed, the ruling is almost irresponsibly vague and general in this respect, given the magnitude of its impact. At the same time, the EU has been working to provide a bit more clarity on the applicable standards through the Article 29 Working Party.[216]

An additional problem with delegating this responsibility to search engines is that it significantly raises the costs and legal complexity of running a search engine. While Google, and some well-funded competitors like Bing, can afford this, the ruling may have served to entrench the competitive advantage that established players enjoy by significantly raising the bar for entry into this market.

[216] "Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12", Article 29 Data Protection Working Party, 26 November 2014. Available at: ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

Criticisms aside, as binding law in Europe, search engines have a duty to implement the right to be forgotten and they should take the human rights impact into account when doing so. Despite the ECJ's failure to afford freedom of expression its proper place in their ruling, this interest should play a strong role in search engines' decision-making about whether to acquiesce to a right to be forgotten request. Given the important impact that the right to be forgotten could have on the character of the Internet, search engines should develop clear and sophisticated policies and decision-making standards regarding requests to block results from searches pursuant to the right to be forgotten ruling. This should, among other things, include an assessment of the various public interest considerations that are likely to weigh on each side of the equation (i.e. in favour of privacy and of maintaining access to information). To this end, search engines should carry out robust consultations with key stakeholders to inform their policies on this issue.

Transparency is also important when implementing the right to be forgotten and search engines should be clear about how their decision making works, including by publishing the policies and policy guidance noted above, along with periodic aggregated information about removal requests and how they were processed.

A third important value is due process. Search engines should promptly inform any party whose content is the subject of a removal request and give them an opportunity to counter the claim, including by arguing that the public interest lies in keeping the information available. For more difficult or cutting edge requests, consideration should be given to putting in place an appeals mechanism or opportunity for more in-depth consideration of the matter. In addition, search engines should avoid taking the easy route, which is just to remove information from search results, given that incentives almost inherently line up this way, and instead undertake a proper and fair consideration of the matter. Should the matter go back to the courts, search engines should argue that their responsibility is limited to reaching a reasonable decision rather than getting the matter right, in the sense of coming to the same decision as a court might after a full hearing on the matter (which search engines obviously cannot do for each case). In legal terms, this means that their decisions should simply be subject to a judicial review standard.

Finally, given the troubling elements of the right to be forgotten as set out in the ECJ ruling, content providers should explore avenues to push back as far as possible. The websites of several media outlets, such as the BBC and The Telegraph, have sought to limit the negative impact of the right to be forgotten by maintaining special lists on their websites of any material which has been removed from searches, including links to the original articles and descriptions of the content.[217]

[217] Neil McIntosh, "List of BBC web pages which have been removed from Google's search results", BBC, 25 June 2015, available at: www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379; and Rhiannon Williams, "Telegraph stories affected by EU 'right to be forgotten'", The Telegraph, 3 September 2015, available at: www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html.

Google's decision to appeal against an order by a French court that it apply blocks carried out under the right to be forgotten globally to all of its websites, as opposed to just to European websites, is another welcome move.[218]

[218] Julia Fioretti and Mathieu Rosemain, "Google appeals French order for global 'right to be forgotten'", Reuters, 19 May 2016. Available at: www.reuters.com/article/us-google-france-privacy-idUSKCN0YA1D8.

Stand Up For Digital Rights

Recommendations for Addressing Privacy Concerns Online:

Communicating With Users

- **Intermediaries should publish clear and transparent information about their policies and practices regarding the collection, processing and sharing of user information and the level of privacy protection they afford their users. This should include a list of the specific types of third parties who may be given access and information about how the information may be used by these third parties. Where policies need to be complex due to the fact that they form the basis of a legal contract with users, they should be accompanied by clear, concise and easy to understand summaries or explanatory guides.**
- **Intermediaries should make sure that any representations they make to users regarding privacy or anonymity are clear and reasonable, and they should then respect those commitments.**
- **Intermediaries should allow their users to view personal information they have gathered or shared which relates to them.**
- **Intermediaries should take reasonable steps to educate their users about security online and should consider introducing incentives to encourage users to adopt good security practices.**
- **Where a security breach occurs, intermediaries should inform their users promptly and fully, particularly anyone whose information has or may have been compromised.**

Data Minimisation

- **Intermediaries should limit the amount of personal user data they collect and store to what is reasonably necessary for operational or commercial reasons.**
- **Intermediaries should make reasonable efforts to limit the ways in which they process personal user data to what is reasonably required to sustain their business models, including by limiting personal data processing to fully automated systems whenever possible.**

- **Intermediaries who rely on a business model whereby users trade their personal information for services should consider offering customers the possibility of opting out of the model in exchange for paying for the service.**
- **Intermediaries should allow users to request that their accounts be permanently deleted, including all information that the intermediary has gathered about them (except where this information has been aggregated or processed with other information and extraction is not practical or it is needed for ongoing operational purposes).**

Securing Data

- **User information should, whenever this is legally, operationally and technically possible, be encrypted and anonymised during storage.**
- **Intermediaries should, whenever possible, support end-to-end encryption.**
- **When releasing data for research purposes, which is a recognised public interest action, intermediaries should make sure that adequate measures have been taken to protect private content in the data, for example through proper anonymisation of the data or by requiring researchers to limit further dissemination of the data.**

Anonymity

- **Intermediaries should take into account the human rights impact of real-name registration policies and should work to mitigate any negative impacts, including by allowing use of pseudonyms or by allowing parts of the service to be used anonymously. Intermediaries should not require real-name registration where this would significantly harm the rights of their users.**

The Right to Be Forgotten

- **Search engines which are subject to the right to be forgotten should publish detailed information about their policies, standards and decision-making processes in assessing removal requests, as well as aggregated information about the number of requests received and how they were processed.**
- **Search engines should develop robust and detailed policies and standards regarding how they apply the right to be forgotten which ensure a proper balancing between freedom of expression and the right to information, on the one hand, and privacy, on the other. They should carry out robust consultations with key stakeholders, including civil society actors, when developing these policies and standards.**

- **Search engines should respect due process when applying the right to be forgotten, including by informing those whose content is subject to a removal request, as far as this is legally permitted, and by giving them an opportunity to argue that the material should not be blocked, including because the public interest lies in continuing to display the content. Consideration should be given to putting in place some sort of appeals or reconsideration mechanism for more difficult or cutting edge cases.**

Key Issues: Transparency and Informed Consent

The Internet has fundamentally changed our relationship with information, raising expectations regarding accessibility and making it vastly more difficult to keep secrets. It is no coincidence, for example, that a rapid expansion in recognition of the right to information coincided with the spread of digital technologies and the rise of the Internet.[219] Consumers have also grown more demanding in terms of openness on the part of private sector intermediaries, in part as a result of the increasingly powerful role that these actors play in their day-to-day lives. Where users' personal information is being stored and processed, there is also a broadly recognised right to track how this is being done, as was spelled out in the UN Human Rights Committee's General Comment on the right to privacy:

> In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files.[220]

Edward Snowden's disclosures, which exposed private sector involvement in secret government surveillance programmes, provided significant further impetus to calls for greater transparency.

Transparency Reports

It has now become relatively common among major tech firms to publish transparency reports.[221] Although the specific information provided varies between different companies, the central thrust is to profile requests to take down content and government attempts to access user information. Better practice in dealing with takedown requests is to provide statistics broken down into the reason for the request (copyright, hate speech and so on), the type of requester (government, private individual, commercial entity and so on), the date of the request, geographic information about the location of the requester and the uploader, and statistics about how the requests were ultimately disposed of. Information about how often users were notified of the requests, and after what period of time, is also useful. In addition to information about requests for material to be removed, companies

---

[219] A rapid increase in the rate of adoption of RTI laws began in the mid-1990s. See Centre for Law and Democracy and Access Info Europe, RTI Rating Data Analysis Series: Overview of Results and Trends (2013). Available at: www.law-democracy.org/live/wp-content/uploads/2013/09/Report-1.13.09.Overview-of-RTI-Rating.pdf.

[220] Human Rights Committee, General Comment 16, adopted on 8 April 1988. Available at: tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1_Global/INT_CCPR_GEC_6624_E.doc.

[221] See, for example, Google's transparency report: www.google.com/transparencyreport/, Facebook's transparency report: govtrequests.facebook.com/ and Twitter's transparency report: transparency.twitter.com.

should publish material about their own enforcement of their terms of service, such as where content is automatically flagged by a particular algorithm or where users have their accounts deleted for committing some sort of prohibited action.

Open Net Korea

A major problem with South Korea's current situation is that telecoms and broadband providers do not publish any sort of transparency reports. NAVER and KAKAO are the two largest portals and only began transparency reporting in December 2014. Both portals publish surveillance transparency reports, whereas only KAKAO publishes a censorship transparency report. Although Google has produced statistics on the Korean government's surveillance and censorship requests on its global transparency page, its market share in Korea is very small.

Before December 2014, the only statistics available were obtained through private sources or by legislators. These legislators worked with agencies that could make disclosure demands on the private sector intermediaries that were licensed or registered with them. For example, in November 2010, we acquired partial statistics from MP Choi Moon-soon after he obtained information from the Korea Communications Commission, and in October 2012, we obtained similar information from MP Nam Kyung-pil. An important revelation from these statistics was the steady and significant rise in the amount of URL takedowns that were privately requested under Article 44-2 of the *Network Act* for non-copyright purposes. In 2008, NAVER and DAUM, the two largest content hosts, had 70,401 and 21,546 takedowns respectively. In the first six months of 2012, there were 104,578 takedowns by NAVER and 40,538 takedowns by DAUM.

The lack of transparency among telecoms and broadband providers (which receive the majority of the surveillance requests) and poor legal requirements regarding notification results in low public awareness of the vast level of State surveillance that exists and consequently a lack of public engagement on the issue. A positive sign that the present transparency reporting could bring about change is that by producing government surveillance transparency reports, NAVER and DAUM appear to be holding themselves accountable for better performance.

Where possible, companies should publish similarly detailed information regarding the nature and processing of requests by governments for user information. However, this type of reporting can be limited by legal restrictions. In the United States, for example, private sector intermediaries are only legally allowed to disclose information about National Security Letters[222] in highly aggregated ranges

[222] National Security Letters are orders which allow the Federal Bureau of Investigation to demand data and which are subject to a gag order forbidding the recipients from revealing details about their existence.

(for example, between 1,000 to 1,999).[223] These restrictions should be challenged wherever possible. Major tech firms in the US are currently locked in a battle with the government over what they may reveal about their role in mass surveillance schemes.[224] Some firms have found a novel way around this by using 'warrant canaries'.[225] A warrant canary is a statement in a company's transparency report indicating that, within a set time period, it did not receive any government requests for information which were the subject of a gag order. If the company does receive such a request, it can indicate this without breaching the law by removing the statement (i.e. so that is it conspicuously declining to signal that it did not receive any requests).

Christopher Parsons

To be effective, transparency reports should do more than just disclose statistics. They should, ideally, be standardised across an industry so that analysts can understand the full extent of government agencies' attempts to compel or request information from intermediaries. Where companies have wildly different modes of reporting requests it can be impossible to ascertain the actual number of times requests are made, per year, in similar industry categories (such as telecommunications or social media). The consequence is that subscribers and analysts alike can be left without a clear understanding of the actual regularity, scope, or common rationales for data requests.[226]

Transparency reports should also include information concerning a given company's data retention policies. A production order for text messages served on a company that permanently retains all its subscribers' texts will likely produce significantly more data than one relating to a company that operates with a thirty-one day retention period. Providing such information allows individuals to determine the number of records which may be accessible to government authorities. Otherwise, it can be difficult for individuals to ascertain what these retention periods are.[227] Authorities, in contrast, are less likely to run into these

[223] Electronic Privacy Information Center, "National Security Letters". Available at: epic.org/privacy/nsl/.

[224] Ewen MacAskill, "Yahoo files lawsuit against NSA over user data requests", The Guardian, 9 September 2013. Available at: www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests.

[225] "Frequently Asked Questions", Canary Watch. Available at: canarywatch.org/faq.html.

[226] Christopher Parsons, "Restoring Accountability for Telecommunications Surveillance In Canada," The Mackenzie Institute, August 11, 2015. Available at: www.mackenzieinstitute.com/restoring-accountability-telecommunications-surveillance-canada/. Christopher Parsons, "Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports," Social Sciences Research Network, January 14, 2015. Available at: papers.ssrn.com/sol3/papers.cfm?abstract_id=2546032.

[227] In Canada, efforts to learn about intermediaries data retention periods were largely fruitless despite availing themselves to a range of advocacy and legal tactics. For more, see: Andrew Hilts and

knowledge deficits as they can determine record keeping periods by either consulting companies' (private) law enforcement authority guideline handbooks or by speaking with other security and intelligence professionals who have made requests of various private sector intermediaries in the past.

The policies adopted by private sector intermediaries to respond to State agencies' requests are often documented in companies' Law Enforcement Agency (LEA) Guideline handbooks. These sorts of handbooks "include the detailed procedures government agencies must follow to request corporate-held data, the kinds of identification government agencies must present before information will be disclosed, the time for corporations to process requests, and the costs agencies must pay for the requests to be processed."[228] Companies can choose to publish these handbooks and, in the process, clarify to government agencies and subscribers alike "what kinds of data the company stores, for how long, and under what terms it can be (and is) released" while also clarifying to subscribers "exactly how a TSP handles their personal information … when presented with different kinds of court orders."[229] Private sector intermediaries routinely receive requests from foreign State agencies for access to corporate data and these handbooks can also clarify "how the company must process foreign authorities' requests for company-held data, identify whether customers are notified of either domestic or foreign authorities' requests, outline the period of time the company can take to respond to requests, and state whether the costs incurred in fulfilling the government request must be compensated or not."[230]

These handbooks establish what exactly a company retains, for how long, and under what conditions it will disclose particular subscribers' information to government agencies. However, the more common practice is to keep such handbooks or policies confidential rather than opening up their practices to public evaluation. In the US several companies, predominantly Internet companies such as Yahoo!, Microsoft, and Google, have either published their law enforcement guideline handbooks or had them leaked to the public. No Canadian companies have published correspondingly detailed handbooks.

Christopher Parsons. (2014). "Enabling Citizens' Rights to Information in the 21st Century," *The Winston Report*, Fall 2014.

[228] Christopher Parsons, "Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports," Social Sciences Research Network, January 14, 2015. Available at: papers.ssrn.com/sol3/papers.cfm?abstract_id=2546032.

[229] Christopher Parsons, "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," Telecom Transparency Project, retrieved November 17, 2015, pp. 54. Available at: www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[230] *Ibid.*

Terms of Service and Policies

It has become a common joke that nobody reads a company's terms of service. In 2010, as an April Fools Day prank, an online video game retailer inserted a clause into its terms stating that, by accepting, customers acknowledged that the company now owned their soul. 88 percent of customers that day (more than 7500 people) agreed to the terms.[231] Similarly, in June 2014, F-Secure, an Internet security firm, opened a public Wi-Fi connection in London the terms and conditions of which required users to "assign their first born child to us for the duration of eternity".[232] This clause also went largely unnoticed.

Although amusing, the lack of attention given to terms of service is troubling given that these terms serve as the legal basis for the relationship between the company and its users, based on the fact that users formally accept or commit to these terms when signing up for the service.

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

Most private sector intermediaries reserve the right, at their discretion, to remove content proactively when it violates the law or their own terms and conditions. The terms and conditions of these platforms are often long and difficult to understand. It is difficult for users to obtain a complete picture of all the content that can be removed because these rules are often scattered in different sections of one or more documents. Since users are unlikely to read the entirety of a company's terms, it is easy to take an action that would authorise the removal of the content or an account suspension.

The fact that users so rarely pay attention to their content also effectively gives companies a licence to draft these terms incredibly broadly. For many companies, it is difficult for even a careful reader to deduce the practical implications of their terms of service.

For example, Facebook's Data Policy[233] says that it collects information (defined extremely broadly) about users or others, which users provide to Facebook, companies operated by Facebook or third-party partners. The Policy says that this information is used to provide services, personalise content, market to users, conduct surveys and research, show advertisements and promote security across

[231] Joe Martin, "GameStation: 'We own your soul'", bitGamer, 15 April 2010. Available at: www.bit-tech.net/news/gaming/2010/04/15/gamestation-we-own-your-soul/1.
[232] Tom Fox-Brewster, "Londoners give up eldest children in public Wi-Fi security horror show", Guardian, 29 September 2014. Available at: www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause.
[233] Available at: www.facebook.com/full_data_use_policy.

their services. The Policy says that this information can be shared with third-party apps or websites, and that Facebook may share any user information within their family of companies, or to anyone who purchases a part of Facebook's assets or services. The Policy specifies that information shared with advertisers is not personally identifiable (unless the user gives permission otherwise), but goes on to say that information is shared with vendors, service providers, and other partners who globally support their business, noting that these partners must adhere to "strict confidentiality obligations". However, the Policy also says that information may be shared in response to a legal request where required, or if necessary to detect, prevent and address illegal activity. The Policy says that Facebook will retain user information as long as is necessary for its business purposes, or until the user's account is deleted.

These terms grant Facebook incredibly broad licence. The only concrete limitations on the company's actions that they contain are a promise to anonymise information before it is provided to advertisers (unless the user gives permission or the advertisers are considered among the "vendors, service providers and other partners") and an apparent promise that once an account is deleted Facebook will delete information associated with the account.

Some claims within the Policy appear contradictory or misleading. For example, the section on responding to legal requests for user information begins with a statement that information will be shared "if we have a good faith belief that the law requires us to do so" and, in terms of requests from outside of the United States, includes a further caveat that the requests should be "consistent with internationally recognized standards". However, the Policy goes on to say that information may be shared if Facebook has a good faith belief that it is necessary to address or prevent illegal activities, which sets the bar far lower, effectively rendering the statement that requests should be legally binding and in line with international standards meaningless.

The potential breadth of action that Facebook's Data Policy grants the company was laid bare in October 2014, when the company published an academic paper revealing that it had been "experimenting" on its users, in particular regarding how slight changes to their news feed through the site could impact on their political engagement or mood.[234] The idea of a formal, academically-published experiment on 61 million unsuspecting subjects raised concerns, particularly in light of the potential for large-scale social manipulation. The company defended the experiment by noting that it is constantly tweaking its interface and that this was merely a logical extension of routine assessments to determine how to deliver content better. Facebook's Data Policy specifically includes references to academic research. Nonetheless, it is likely that, if users who signed up for a Facebook account were

[234] Micah L. Sifry, "Facebook Wants You to Vote on Tuesday. Here's How It Messed With Your Feed in 2012", Mother Jones, 31 October 2014. Available at: www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout.

presented with a clear, bold message saying that the company intended to use them to carry out social and behavioural experiments, at least a few may have reconsidered the decision.

Although Google's Privacy and Terms are clearer in some ways, they also contain vague elements.[235] For example, they state that user information may be provided to "affiliates or other trusted businesses or persons" in accordance with their Privacy Policy and any other appropriate confidentiality and security measures. Baidu, a Chinese web services company, operates under a User Agreement which is even more vague, saying only that user information "will be utilized to improve the services and web content provided for the user" and shared if required by laws, regulations or relevant government authorities, or to safeguard the company's rights and interests.[236]

Arabic Network for Human Rights Information

Etisalat Egypt, which provides mobile communications services, has terms of contract that stipulate that, "the company is committed to maintain the confidentiality and privacy of subscribers' information, and not to disclose it except under a court order or the implementation of the law or with the consent of the client." However, there is no explanation of what is meant by "the implementation of the law". It also stipulates that service can be cut should the user "[misuse] the service for purposes that may adversely affect the company financially or morally".

STC, one of Saudi Arabia's largest telecommunication companies, also uses vague and unclear contracts, including terms and conditions which provide that "the customer is committed not to misuse services in a detrimental way for the company or one of its clients or a breach of public morality or use it for non-intended purposes. In the case of a breach, the company may take the necessary steps to address it" including potentially cutting off service. There are no examples of what constitutes "harm" or "public morals" or "abuse" or any clarifying definitions whatsoever. Furthermore, there is no information available on the website informing the user of the extent of data collection about the user or the circumstances under which this information may be disclosed.

The lack of public understanding of what, exactly, these terms and policies contain is particularly problematic since it undermines the core dynamic whereby users trade their privacy for services. The legality of this exchange is predicated on informed consent by the users regarding how their information will be collected, processed and disclosed. Where a company's terms or policies are written impossibly broadly,

[235] Available at: www.google.com/intl/en/policies/privacy.
[236] Available at: motu.baidu.com/protocal.html.

or in a deliberately confusing fashion, it is difficult to see how meaningful consent can exist.

This is not to minimise the legitimate challenge that private sector intermediaries face in engaging users on these issues. Some policies require users to scroll through to the end of the document before they can indicate their acceptance, while others highlight important aspects of the policy with larger or differently coloured text, and/or subdivide the agreement into a series of thematic screens which must be clicked through individually. There is no indication, however, that any of these measures are particularly effective in getting users actually to read and understand the terms. This is likely because the measures do nothing to solve a key underlying problem, which is that terms of service are usually long and difficult for a lay person to understand even when they are not written in a deliberately misleading manner. An active digital citizen may sign up for several services a week and as a result be presented with potentially hundreds of pages of legal documents.

A welcome move by some companies is to provide a simplified version of their terms of service. Disconnect, a search engine, prefaces their privacy policy with four simple statements:

> Nothing in this policy contradicts the following statements:
> 1. We don't collect any of your personal info, including your IP address, other than information you voluntarily provide.
> 2. We don't sell your personal info to advertisers or other third parties.
> 3. We share your personal info only when legally required, or when reasonably necessary to prevent harm in an emergency situation.
> 4. We retain your personal info, excluding info you make public, for no more than 30 days after you request deletion.[237]

Ultimately, there is a strong need for a common framework which would allow users to understand a company's policies clearly and with only a reasonable effort, and to compare them with those of competitors. One interesting approach is that taken by Creative Commons, which uses symbols to simplify dramatically the standards for releasing material publicly. Creative Commons offers users a "menu" of options which can be understood with minimal effort and which allows users to understand relatively complex terms easily. Although the subject matter that Creative Commons deals with is far simpler than what needs to be conveyed in many terms of service, there are indications a similar approach may be possible. One interesting initiative, "Terms of Service; Didn't Read", provides short summaries of the main points of the terms of service agreements offered by major tech services.[238] Important clauses are explained in plain language and rated on a five-point scale according to how concerned users should be about them. Disconnect embeds icons in its search results, allowing users to assess quickly and easily

[237] Available at: disconnect.me/privacy. Accessed 30 May 2016.
[238] Available at: tosdr.org/.

whether the websites comply with Do-Not-Track (DNT) requests, support encrypted connections, retain user data for long periods of time and so on.[239]

Beyond clear language, accessibility is important. Information should be posted in a visible and prominent manner, and should be posted in each of the languages in which they offer services. Where possible, this information should be consolidated, so that users do not have to navigate through a maze of different, and potentially contradictory, documents in order to obtain clear information.

Marketing and Advertising

Misleading or deceptive marketing practices are a problem in the tech world as they are in the offline world. AT&T, for example, faced a lawsuit from the United States Federal Trade Commission after they instituted throttling measures against millions of customers once they reached a particular ceiling, even though they had purchased an "unlimited" data plan.[240] AT&T defended itself, in part, by claiming that the term "unlimited" had different meanings for different companies, highlighting the lack of a standardised yardstick. The rapidity at which new tech products continue to evolve means that there is a clear need to ensure that users are clearly informed about what to expect from a product or service. This is compounded by the fact that, since many products are offered free of charge, users may not be as wary as they would if they were spending money.

In the rapidly changing digital economy, many private sector intermediaries face pressure to pull existing users into their newest product offerings. This raises obvious questions about consent and better practice is for private sector intermediaries to make new services opt-in, rather than opt-out.

Clear communication is particularly important where speech is being restricted or content is being removed. Users need to be able to understand why and how rules are applied, so that they can attempt to stay on the right side of them. For years, Reddit had a policy of not informing suspected spammers that they had been banned from posting to the site, in order to prevent spam programmes from figuring out how they were being identified. The resulting "shadowban" meant that to a user their posts appeared to go through successfully but they were invisible to everyone else. In May 2015, a user complained that he had been mistakenly banned for three years without even realising it.[241] Later that year, in response to a broad push for

[239] Available at: disconnect.me/icons.
[240] John P. Mello Jr., "AT&T: We Told Our Customers 'Unlimited' Doesn't Mean 'Unlimited'", Commerce Times, 29 October 2014. Available at: www.ecommercetimes.com/story/81275.html.
[241] See: "TIFU by posting for three years and just now realizing I've been shadow banned this entire time", Reddit, 6 May 2015. Available at: www.reddit.com/r/tifu/comments/351buo/tifu_by_posting_for_three_years_and_just_now/.

more transparency, the website announced that it was transitioning to account suspension, which is more readily visible to the subject.[242]

[242] "Account suspensions: A transparent alternative to shadowbans", Reddit, 10 November 2015. Available at: www.reddit.com/r/announcements/comments/3sbrro/account_suspensions_a_transparent_alternative_to/.

Stand Up For Digital Rights

Recommendations for Transparency and Informed Consent:

Transparency Reporting

- **Intermediaries should produce regular transparency reports which include, at a minimum:**
  - **Statistics on the number of takedown requests received, broken down by category of request, by type of requester, by the date and subject of the request, and by the location of the requester.**
  - **Statistics on the number of requests received for information about users, broken down by category, by type of requester, by date and by the location of the requester.**
  - **Information about actions intermediaries have taken proactively to enforce their terms of service, including statistics about material removed and accounts deleted.**
- **Intermediaries should publish detailed information about their procedures for responding to requests from law enforcement agencies, as well as their procedures for processing other government requests to restrict content, block services or deactivate accounts.**

Terms of Service

- **Intermediaries should take steps to ensure that their terms of service are clear to users, for example by publishing clear, concise and easy to understand summaries or explanatory guides.**
- **Intermediaries should publish their terms of service in each of the languages in which they offer services, and post this information prominently on their website.**
- **Intermediaries should support initiatives which aim to enhance understanding of their terms of service, such as "Terms of Service; Didn't Read", and implement measures to try to get users actually to read them.**
- **Intermediaries should consult with users prior to major amendments to their terms of service, notify users of amendments to their terms of**

service and make previous versions available online so that users can assess the changes.

- **Intermediaries should provide reasonable avenues of engagement for users seeking clarification of their terms of service and allow users to propose changes.**

Other Issues

- **Intermediaries should publish information about how their terms of service apply in different jurisdictions.**
- **Intermediaries should challenge legal restrictions on what information they can release about takedown and user information requests, and should explore alternative avenues to facilitate disclosure, such as the use of warrant canaries.**
- **Intermediaries should not automatically opt their users into new services.**
- **Intermediaries should be careful to avoid misleading promotional material, taking into account the rapidly evolving nature of the services that are being offered, which means that it is difficult for established industry meanings and understandings to evolve.**

Key Issues: Responding to State Attacks on Freedom of Expression

Many private sector intermediaries face the challenge of what to do when confronted by government demands which do not accord with international human rights standards. The responsibility to avoid complicity in human rights violations is a key part of the UN's Protect, Respect and Remedy framework:

> 73. The corporate responsibility to respect human rights includes avoiding complicity. The concept has legal and non-legal pedigrees, and the implications of both are important for companies. Complicity refers to indirect involvement by companies in human rights abuses – where the actual harm is committed by another party, including governments and non-State actors. Due diligence can help a company avoid complicity.
>
> 74. The legal meaning of complicity has been spelled out most clearly in the area of aiding and abetting international crimes, i.e. knowingly providing practical assistance or encouragement that has a substantial effect on the commission of a crime, as discussed in the 2007 report of the Special Representative. The number of domestic jurisdictions in which charges for international crimes can be brought against corporations is increasing, and companies may also incur non-criminal liability for complicity in human rights abuses. [references omitted][243]

How companies should respond to government demands which harm freedom of expression is the main issue the GNI focuses on. The GNI makes it clear that it does not expect companies to refuse to comply with domestic laws and instead focuses on engagement with governments to encourage them to adopt laws and policies which are in line with international freedom of expression standards. The GNI's Implementation Guidelines state that companies should require governments to follow established domestic legal processes when restricting freedom of expression and that companies should interpret any demands that such restrictions make on them in a manner which is minimally intrusive to freedom of expression. The GNI Implementation Guidelines also say that companies may legally challenge restrictions or demands which do not comport with human rights standards, but ultimately stresses that this decision lies at the discretion of the companies themselves:

> It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on freedom of expression,

[243] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, 7 April 2008. Available at: www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-report-7-Apr-2008.pdf.

the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.[244]

After the Snowden revelations, the Electronic Frontiers Foundation (EFF) withdrew from the GNI and developed its own, stronger and more specific set of standards regarding how companies operating in the United States should respond to government requests.[245] These standards hold that companies should only hand over user information when confronted by a legal warrant, should publish regular transparency reports on these requests and should publish guides which explain their internal procedures for responding to government requests. The EFF standards also ask companies to provide notice to users about a government request before it is responded to, when that is legally permitted. In cases where they are prohibited from informing the user right away, the EFF calls on companies to commit to notifying the user as soon as this is legally permitted.

Arabic Network for Human Rights Information

Egypt's Telecommunications Act does nothing to protect the privacy and personal data of Internet users, and instead is focused on guaranteeing that the authorities can access any information or data they desire. Article 64, for example, prohibits telecommunications service providers and users from using encryption systems in their conversations, and forces Internet service providers to provide the means necessary for national security bodies and the armed forces to obtain information about their users. Telecommunications companies in Egypt cannot get licenses without allowing the military and security services to access the personal data of their users, including to spy on political activists.

Vodafone, a company that provides telecommunications and Internet services in Egypt, publicly announced that Egyptian law allows the national security services and the military to conduct surveillance of communications, and disclosed that they were being forced to cooperate with the security services under Article 64 of the Telecommunications Act, as well as Article 95 of the Code of Criminal Procedure. The company also mentioned the existence of secret wires connected directly to its network and the networks of other mobile operators which allowed government agencies to eavesdrop and record conversations of users and, in some cases, track their whereabouts.

[244] Global Network Initiative, Implementation Guidelines for the Principles on Freedom of Expression and Privacy. Available at: globalnetworkinitiative.org/sites/default/files/GNI_-_Implementation_Guidelines_1_.pdf.

[245] These standards are available at: www.eff.org/who-has-your-back-government-data-requests-2015#best-practices. Although the standards focus primarily on data protection and privacy, they also deal with content removal requests.

The Dynamic Coalition on Platform Responsibility (DCPR), in its *Recommendations on Terms of Service and Human Rights*, suggests that companies should only comply with requests which are grounded in a "legitimate" law or regulation, defined as follows:

> Laws and regulations are procedurally legitimate when they are enacted on the basis of a democratic process. In order to be regarded also as substantively legitimate, they must respond to a pressing social need and, having regard to their impact, they can be considered as proportional to the aim pursued.
> (a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);
> (b) It must pursue a legitimate purpose (principle of legitimacy); and
> (c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).
> If it is manifest that the measure would not pass this three-pronged test, the platform operator should deny the request and, to the extent possible, challenge it before the relevant court. [references omitted][246]

Christopher Parsons

In 2012, Google began warning a subset of its users that they might be the targets of State-sponsored attacks by inserting a warning notification at the top of their screens when they log into Google services. Google is well situated to analyse such attacks and provide the warnings because of the company's ability to analyse and investigate incoming malware and phishing attacks. Facebook also started issuing similar warnings as of October 2015. The notifications from these companies are important because few individuals are able to understand whether a particular phishing, spearphishing or malware attack originates from a commercial, State or other actor. Moreover, the warnings can help individuals to correlate other abnormal activities with a similar threat actor or set of actors. In effect, these companies' investigations and warnings can help individuals realise the threats facing them and subsequently try to adjust their behaviour to reduce their risks.

However, these notifications systems also highlight that the precise methodologies that are used to determine who is responsible for an attack are not well publicised. The heuristics or analysis or investigatory techniques that go into determining whether an attack is State sponsored thus cannot be directly analysed and validated (or refuted) by the broader security community. Further, the notices do not indicate which country is engaged in these sorts of sponsored attacks, or whether US-based companies would notify individuals of a US government-sponsored attack or just of attacks sponsored by foreign governments. Notably, the attacks that Google and Facebook alike notify users about are limited to 'hacking' attempts; subscribers whose data is requested using a lawful access tool do not receive notifications. The

[246] "Recommendations on Terms of Service and Human Rights", Dynamic Coalition on Platform Responsibility. Available at: review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-platform-responsibility-dc-pr/.

result is that even the 'best of breed' analysis and investigation systems that inform specifically affected subscribers have significant deficits.

Beyond notifying specific individuals that they have been targeted by a State actor using malware or other attack tools, companies can try and notify individuals whose data is requested by such agencies. Subscribers rarely learn of requests to access their data by government agencies, unless they are subsequently charged with an offence. As a result, their personal information can be captured by government agencies, and used or disseminated amongst such agencies, entirely without their consent or even knowledge. And, where a charge is not brought against the individual, they may never have an opportunity to contest the legitimacy of the government possessing - or having requested - the information in the first place. Only private sector intermediaries are in a position to know whether a subscriber's information has been requested. As a result, a powerful way for private sector intermediaries to facilitate transparency surrounding State-driven surveillance is to commit to informing subscribers about such requests.

Some of the most challenging cases of private sector complicity in human rights violations involve China, which has an abysmal freedom of expression record as well as a large and rapidly growing population of Internet users. The country has been particularly bold in taking action against companies that refuse to acquiesce to their demands, including by blocking them from the lucrative Chinese market.

In addition to complying with censorship demands associated with China's "Great Firewall", there have been allegations that major tech firms were directly complicit in assisting the Chinese State to prosecute journalists.[247] There have even been instances of private sector actors being utilised as weapons of cyber war. In March 2015, reports emerged of an enormous distributed denial of service (DDoS) attack being mounted against GitHub, a website which, among other projects, provides access to tools to subvert China's censors.[248] Analysis of the attack revealed that it originated from servers of the popular Baidu search engine, redirecting users of the site to participate in the attack against GitHub, although Baidu strenuously denied complicity.[249]

Although China is the most high profile example, companies face similar dilemmas in other countries. Both Twitter and Facebook have faced substantial criticism for

[247] Joseph Kahn, "Yahoo helped Chinese to prosecute journalist", The New York Times, 8 September 2005. Available at: www.nytimes.com/2005/09/07/business/worldbusiness/07iht-yahoo.html.
[248] Sebastian Anthony, "GitHub battles 'largest DDoS' in site's history, targeted at anti-censorship tools", Ars Technica, 30 March 2015. Available at: arstechnica.com/security/2015/03/github-battles-largest-ddos-in-sites-history-targeted-at-anti-censorship-tools/.
[249] Bill Marczak and Nicholas Weaver, "China's Great Cannon", Munk School of Global Affairs, 10 April 2015. Available at: citizenlab.org/2015/04/chinas-great-cannon/.

removing content in Pakistan,[250] while telecoms companies operating in Ethiopia have faced scrutiny for facilitating the country's invasive surveillance and censorship programmes.[251] Moreover, abusive government demands can also be made in free and open democracies. In 2010, Amazon, a major United States-based web hosting company, cut off the Wikileaks website from its platform after a United States Senator complained directly to them about Wikileaks' disclosures.[252] The United States-led mass surveillance programmes, which relied heavily on private sector intermediaries, are another example of an abusive practice taking place in a developed democracy. This also demonstrates the secrecy in which even pervasive systems can operate. It is safe to assume that for every well-publicised case of an intermediary acquiescing to State demands which violate the rights of their users there are many more which pass under the radar screen.

Ultimately, Google is not responsible for bringing democracy to China and Twitter is not responsible for promoting tolerant secularism in Pakistan. However, private sector intermediaries do have a duty to avoid complicity in abuses carried out by the governments of the countries where they operate. Ideally, these considerations should begin with a human rights impact assessment before a new market is entered, or a new product is launched. Private sector intermediaries should develop strategies to mitigate any risks identified, for example by disabling particular features which may be prone to misuse in a particular national context or by avoiding locating their employees or storing data in countries which have a poor record of respecting freedom of expression or the right to privacy.

No government, of course, has a perfect human rights record. What constitutes a legitimate restriction on freedom of expression is complex and different countries have different rules in areas such as privacy, obscenity, defamation, hate speech and so on. As a result, by and large, it is reasonable to expect private sector intermediaries to comply with local laws on these issues in the jurisdictions where they operate, even if those laws may deviate from international human rights standards. For example, Canada has a criminal defamation law on the books, which includes possible prison terms. This runs counter to international human rights standards, which hold that defamation should be treated as a civil, rather than a criminal, matter and that imprisonment is never a legitimate response to defamation. However, if a Canadian judge authorised a warrant for user information

[250] Robert Mackey, "Twitter Agrees to Block 'Blasphemous' Tweets in Pakistan", The New York Times, 22 May 2014, available at: www.nytimes.com/2014/05/22/world/asia/twitter-agrees-to-block-blasphemous-tweets-in-pakistan.html?_r=2; and Declan Walsh and Salman Masood, "Facebook Under Fire for Temporarily Blocking Pages in Pakistan", The New York Times, 6 June 2014, available at: www.nytimes.com/2014/06/07/world/asia/pakistan-facebook-blocked-users-from-political-pages-and-outspoken-rock-band-laal-against-taliban-.html?_r=1.

[251] Arvind Ganesan, "They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia", Human Rights Watch, 25 March 2014. Available at: www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia.

[252] Ewen MacAskill, "WikiLeaks website pulled by Amazon after US political pressure", The Guardian, 2 December 2010. Available at: www.theguardian.com/media/2010/dec/01/wikileaks-website-cables-servers-amazon.

related to a criminal defamation investigation, it seems reasonable to expect an intermediary to comply with the order. On the other hand, one would hope that a similar request in Azerbaijan, where the government is notorious for using criminal defamation laws to target journalists and other critical voices, might raise a red flag.

Although the line can be difficult to draw, where an intermediary encounters a case of their systems or services being subverted to support a clear and grave violation of human rights, they have a responsibility to take action to avoid or mitigate complicity. This can include refusing to turn over records that support a political prosecution or to participate in widespread systems of repression, such as China's Great Firewall. It is worth noting that most global tech companies only maintain a physical presence in a few countries. Outside of those States, governments have no real legal means to compel compliance with their demands, other than by threatening to deny the company access to their market. Twitter, for example, only has assets or employees in the United States, the United Kingdom, Ireland, Japan and Germany, so the government of Pakistan would have no power to seize their property or jail their employees. The only possible sanction that Twitter would face for failing to obey an order of the Pakistani government would be to be blocked in that country.

Open Net Korea

South Korea has a vast State surveillance system over the Internet, which was brought to the public's attention by a major civil society lawsuit. Domestic companies' policy of demanding real names from new users, along with their resident registration numbers, exacerbated this by making accounts easily traceable. As a result, South Korean users began to switch from domestic private sector intermediaries to foreign ones outside the reach of South Korean warrants. Similarly, when the Prosecutors' Office announced plans to search and seize messages from Kakao Talk, the leading chat app in South Korea, for the purpose of investigating defamation of public officials, users began migrating to the foreign chat app Telegram, which provides device-to-device encryption. As the exodus grew, DAUM-KAKAO, the operator of Kakao Talk, announced in October 2014 that it would no longer comply with any wiretap order on chat messages, citing technical challenges with fulfilling the requests for real-time information. Although the exodus itself was not directly related to wiretap orders, consumer privacy concerns were appeased by this publicity stunt, along with two actual shifts in policy, namely that Daum-Kakao began publishing the country's first transparency report on surveillance requests and takedown requests and also began offering the option of device-to-device encryption. This led to its competitor Naver following suit. A year later, when their market position had stabilised, Daum-Kakao's non-compliance policy was retracted.

Being shut out of a country is obviously not a consequence to be taken lightly, given the very real commercial implications this has. And acting ethically with that result may not be very useful in practice, since the company's market share may simply be taken over by less scrupulous competitors. However, where clear abuses of human rights are involved, companies cannot simply wash their hands of complicity any more than merchants selling conflict diamonds can. If the major players put up a unified front in support of human rights, it would be difficult for a country to ban them all (although China may be an exception to this, due to the size of its internal market and its capacity to replace services with home-grown versions). This would also send a powerful message to users that companies are willing to defend their interests. Relevant factors to take into account when determining whether a violation is significant enough to warrant noncompliance with domestic law include the number of users impacted, the severity of the interference, and the broader human rights context in which the interference takes place, including the country's overall human rights record.

Where a State-mandated interference does not qualify as a clear and grave violation of human rights, private sector intermediaries should only hand over information when subject to a legal requirement to do so and should notify users who are subject to a government request as soon as this is legally allowed. Where realistic legal avenues for contesting problematic laws or policies exist, private sector intermediaries have some responsibility to launch legal challenges in appropriate cases and to stand up for the rights of their users. Private sector intermediaries should additionally explore their options for seeking external leverage to support their position, such as soliciting diplomatic support from their home government (particularly if they are based in the United States) or from intergovernmental organisations. In seeking to mobilise against problematic policies, it may be important for intermediaries to liaise with one another and communicate clearly, in order to establish a unified front.

Stand Up For Digital Rights

Recommendations for Responding to State Attacks on Freedom of Expression:

Assessing Risks

- **Intermediaries should carry out thorough human rights impact assessments before making any significant changes that could impact human rights, such as the launch of a new product or entry into a new market, and develop strategies to mitigate any identified risks.**

Communicating With Users

- **Intermediaries should publish guides which explain their internal procedures for responding to requests for them to take action, including by providing information on users, from State actors.**
- **Intermediaries should offer specific guidance to human rights activists, or other oppressed groups, among their user base in countries where specific threats to these groups exist.**

Pushing Back

- **Intermediaries should only hand over user information when legally required to.**
- **Intermediaries should notify users who are the subject of a request from a State actor as soon as they are legally allowed to.**
- **Intermediaries should explore reasonable other avenues to push back against demands from State actors which violate human rights, including seeking diplomatic support from their home governments and intergovernmental organisations and partnering with other intermediaries in order to present a united front against problematic laws, policies or practices.**
- **Intermediaries should, in appropriate cases and where these have a realistic chance of success, pursue legal options to contest abusive laws or policies and support advocacy to change oppressive laws or policies.**

- **In more extreme cases of clear and grave violations of human rights, intermediaries should consider their options carefully, including refusing to obey even legal orders to act which would implicate them in serious human rights abuses and stopping operations in countries where their operations lead to them being complicit in serious abuses.**