Stand Up For Digital Rights!

Recommendations for Responsible Tech

Executive Summary

Introduction[1]

Recent years have seen the formation of new 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 over online communications has increasingly important implications. The enormous impact their policies and practices have on the exercise of key rights like freedom of expression, privacy and the right to political participation has meant that 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 (intermediaries), which we define as private sector bodies whose online operations somehow facilitate communication between two or more parties over the Internet. States are the primary obligation holders for ensuring respect for human rights and the policies and practices of online intermediaries can be heavily influenced by State policies and actions. It is now recognised, however, that private sector actors also

[1] 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, OpenNet 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. For more information about this project, please visit www.responsible-tech.org.

have a direct responsibility to respect human rights and this Report focuses exclusively on the question of how online intermediaries can and should behave.

Background Issues

Human Rights and the Internet

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 and to take part in cultural life, among others. The UN Human Rights Council and the UN General Assembly have both affirmed that human rights standards apply to the online world. The Internet supports human rights by improving communications and information sharing, providing a voice for human rights defenders, and strengthening democratic society through its contribution to political, social, cultural, and economic development. Its importance to human rights has led to calls for access to the Internet itself to be considered a human right, with a concomitant obligation on States to promote universal access to the Internet.

The growth of the Internet and its centrality to many aspects of modern life is starting to affect our understanding of certain rights, especially the evolving dynamic between the right to privacy and the right to freedom of expression. The rise of the Internet has impacted significantly on the balancing of these rights by expanding the expressive sphere, often at the expense of traditional notions of privacy. Due to the ubiquity and special nature of digital technologies, people are choosing to share more information about themselves than ever before. Despite this, a significant proportion of the personal information which is collected and shared is done so without the meaningful consent of the data subject. The impact on privacy of this explosion in the distribution and collection of personal information is compounded by the permanence and accessibility of online information.

Despite this growing challenge to privacy, efforts to protect privacy online can pose a risk to freedom of expression online. This represents, in part, the online reflection of historic tensions between these two rights. But it is complicated by the fact that many of the online tools which facilitate enormous expressive benefits are based on an economic model which seriously undermines privacy. In this way, the Internet has raised the stakes in traditional conflicts between freedom of expression and privacy.

States have positive obligations to take action to ensure that people can enjoy and exercise their rights, including when the threat to those rights comes from private actors. And this applies to both freedom of expression and privacy in an online context. However, intrusive government regulation of the online world is not a desirable solution for either human rights or the private sector. As a result, the

private sector has both a greater responsibility and some motivation to put in place policies and practices that respect human rights.

Human Rights and Private Online Intermediaries

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. The most high profile work in this regard is the 2011 *Guiding Principles on Business and Human Rights*,[2] developed under the auspices of the United Nations. 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. However, even if one assumes maximum goodwill on the part of the private sector, the scope of corporate responsibility is tricky to define, particularly in areas where human rights conflict with profits.

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, the Internet's power is that it facilitates speech directly by individuals, giving everyone a platform and access to a global audience. By the same token, however, this grants the companies which provide these platforms 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 putting unprecedented pressure on online intermediaries to facilitate 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. This has included the launch of major initiatives such as the Global Network Initiative[3] and the Ranking Digital Rights Project.[4] Major international institutions have also issued publications affirming the responsibility of online intermediaries to respect human rights norms, such as the European Commission's *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*[5] and the UNESCO publication, *Fostering Freedom*

[2] 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.

[3] See: www.globalnetworkinitiative.org.

[4] Rebecca Mackinnon, "The Ranking Digital Rights 2015 Corporate Accountability Index is now online!", Ranking Digital Rights, 3 November 2015. Available at: rankingdigitalrights.org/.

[5] 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.

Online: The Role of Internet Intermediaries.[6] Another project of note is the *Manila Principles on Intermediary Liability*,[7] which were developed by a coalition of civil society groups and which focus on the obligations and responsibilities of both States and intermediaries in relation to takedown requests and the disclosure of user information.

Promoting human rights at the State level is by no means a simple task, but efforts to promote respect for human rights among online intermediaries are, in many ways, even more complicated and challenging. Human rights principles, as well as 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, while the presence of strong competition tends to undermine such solidarity among private companies.

There are three layered challenges which any initiative to promote good practice in the private sector faces. The first is engagement, simply getting major private sector actors to the table. The second is transparency, in terms both 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: convincing companies to amend policies or practices which are problematic. These are significant challenges but the human rights community must address them if it is to promote greater respect for human rights by corporations.

Key Issues: 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. Indeed, access to the Internet is increasingly being recognised as a human right.[8] Important access gaps have emerged in the past decades. These include a significant divide in penetration rates between developed and developing countries, between urban and rural populations, and, most importantly, between the better off and the poor.[9] These discrepancies are the result of various factors, such as the cost of purchasing access, the challenge of providing the necessary infrastructure, which creates various cost differentials, especially between urban and rural areas, social challenges that undermine demand, which in turn inhibits the Internet's spread, and sometimes even regulatory approaches that hinder the expansion of Internet access,

[6] UNESCO, "Fostering Freedom Online: The Role of Internet Intermediaries", 2014. Available at: unesdoc.unesco.org/images/0023/002311/231162e.pdf.
[7] 24 March 2015. Available at: www.manilaprinciples.org.
[8] 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.
[9] 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.

either by design or because of a lack of understanding about how the Internet works.

Intermediaries can take various steps to overcome these hindrances and facilitate the spread of Internet access. To help overcome cost barriers relating to access, Internet access providers should invest a proportion of their profits in expanding Internet access, for example through supporting programmes to provide free access to new users or subsidised access for poor households. They should also work to mitigate or eliminate pricing differentials between rural and urban customers. Where the cost of this is high, measures such as providing slower or capped access for rural users are preferable to not providing access at all, or pricing the service beyond consumers' ability to pay. All online intermediaries, but especially content and software providers, should support access by underserved communities by promoting the development of content in less connected communities or smaller languages, and by adopting the World Wide Web Consortium's Web Content Accessibility Guidelines to facilitate access by the disabled.[10]

State-mandated measures to cut off or deny service to users are highly intrusive and are 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 to cutting off access. Providers should also resist these demands as far as possible, including by not implementing them unless confronted with a clear and binding legal instruction to do so. Finally, access providers should, as far as this is legally permitted, be transparent about requests they receive to cut off access.

Key Issues: Net Neutrality

As the Internet has grown, and become more lucrative, this has sharpened the ongoing debate about the foundational principle of network neutrality. The core idea behind this principle is that intermediaries should not favour or disfavour (discriminate against) the transmission of certain types of Internet traffic.[11] 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.

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. However, certain fundamental principles should guide decision-making about this. First and foremost,

[10] World Wide Web Consortium (W3C), Web Content Accessibility Guidelines 2.0, 11 December 2008. Available at: www.w3.org/TR/WCAG20/.

[11] 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/.

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 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 fully respect the principle of network neutrality.

A particularly contentious aspect of the net neutrality debate concerns zero rating projects, 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.[12] Although it can be argued that the harm inherent in zero rating schemes is outweighed by their benefit in bringing new people online, other projects providing a similar "on ramp" to the Internet do not compromise net neutrality. As a result, the onus is on intermediaries proposing or running zero rating schemes to demonstrate that these programmes are clearly more effective in terms of bringing people online than other access schemes which respect net neutrality, and that the benefits are significant enough to justify making compromises to the principle of net neutrality.

Key Issues: 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. However, the sense of anonymity that is associated with being behind a computer or mobile screen can also encourage people's darker impulses. The Internet can be 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. However, their growing influence has placed them under increasing pressure, including from their own users, to mitigate the less desirable aspects of online speech. Gender-based harassment is notoriously endemic online, though it is only part of a broader "civility" problem which has led to a trend towards more active content management by some intermediaries. This,

[12] 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/.

in turn, has given rise to difficult challenges in determining when and how forcefully to intervene.

Some intermediaries will want to set their own standards for acceptable content. In this case, they should ensure that users can understand these policies and practices by posting, in a prominent place, clear, thorough and easy to understand explanations of when and how they take action in relation to content. Where these involve complaints mechanisms, intermediaries should only follow up on complaints where complainants indicate what rule the content allegedly violates. Intermediaries should carefully scrutinise complaints and should be consistent in applying their policies. They should also track frivolous complaints and scrutinise more carefully complaints which come from users who are known to abuse the system.

Although intermediaries have little control over what material is prohibited by law, there are significant differences in how this content is dealt with. 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. It is understandable that intermediaries will wish to shield themselves against legal liability. However, many intermediaries take actions which go significantly beyond the minimum requirements to avoid liability. These include initiatives to target the spread of child sexual abuse imagery, hate speech and copyright infringement. However, experience suggests that these systems are 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 person or organisation finds embarrassing or inconvenient. Automated systems to flag copyrighted material have been found to make mistakes, and are additionally problematic insofar as they are unable to take into account possible defences to copyright infringement, such as fair use.

In order to combat misuse, actions to address problematic content 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 clearly in the policy. Ideally, intermediaries should consult with their users when determining such policies.

Users whose content is subject to removal should, whenever this is legally permissible, be notified promptly and provided with information about the process and their opportunities to mount a defence. Intermediaries should also try to implement solutions to problematic content 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 may be pending, and should offer users the option to preserve and export their data, unless the material is patently illegal.

Addressing Privacy Concerns Online

The right to privacy is recognised internationally as a human right, guaranteed in the *Universal Declaration of Human Rights*,[13] the *International Covenant on Civil and Political Rights*,[14] the *American Convention on Human Rights*[15] and the *European Convention on Human Rights,*[16] as well as in most national constitutions. Privacy is also closely linked to the fulfilment of the right to freedom of expression. The Internet has had a dramatic impact on our understandings of the very concept of privacy, providing unprecedented levels of freedom and anonymity while simultaneously subjecting users to intense levels of tracking and surveillance.

The collection and sale of personal information are major economic forces underlying the spread of Internet services. This has both positive and negative aspects, and States have a responsibility to protect consumers in these relationships.[17] 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 understand that information will be tracked in an automated or aggregated way for advertising purposes, but not expect it to be examined by human beings. Companies which explicitly market the privacy features of their services have a particular obligation to avoid privacy intrusive behaviour.[18] The increasing involvement of third party data brokers in collecting and processing users' information is another cause for concern, due to the opacity of these processes and the lack of any direct relationship between users and data brokers.

A concrete manifestation of users' frustration with intrusive online tracking and advertising is the rise in popularity of ad blocking software, which represents a serious challenge for intermediaries whose business model is based on advertising. Intermediaries should publish lists of the specific types of third parties with which they may share user information and a description of how this information may be used. Intermediaries should also allow their users to view personal information they

---

[13] UN General Assembly Resolution 217A(III), 10 December 1948.
[14] UN General Assembly Resolution 2200A(XXI), 16 December 1966, in force 23 March 1976.
[15] Adopted 22 November 1969, O.A.S. Treaty Series No. 36, to force 18 July 1978.
[16] Adopted 4 November 1950, E.T.S. No. 5, to force 3 September 1953.
[17] 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: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en.
[18] 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.

have gathered or shared which relates to them. They should also grant users the right 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 and extraction is not practical or the information is needed for ongoing operational purposes.

Some intermediaries have legitimate reasons for requiring real-name registration, but 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.

Anonymisation tools can be very important to protecting online privacy. Among many online communities, there is a strong taboo against publishing personally identifiable information about a person using an online alias.[19] Anonymity is particularly important for facilitating communication about sensitive subjects, such as sexual or mental health issues and child abuse, and for enabling whistleblowing. The centrality of the Internet to sensitive communications means that failures on this front can have particularly stark consequences. 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. Perceptions, and building realistic expectations, are of cardinal importance in this area.

Another means of protecting user privacy is through strong data security measures and the use of encryption. Online intermediaries should facilitate and promote the use of encryption, including by storing user information in encrypted formats whenever this is operationally and legally possible and by supporting end-to-end encryption for users. Intermediaries should also consider other means to encourage users to employ strong data security measures, potentially through offering inducements. They should also minimise the amount of data that they hold, since the more information an organisation stores, the greater the risk of a security breach.[20] 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 minimising the risk of damage.

In 2014, the European Court of Justice (ECJ) recognised the right to be forgotten, granting EU citizens a right to request that search engines not display results relating to them which are "inadequate, irrelevant, or no longer relevant, or

[19] 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.
[20] 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.

excessive in relation to the purposes for which they were processed".[21] There are significant problems with this judgment, particularly its failure to consider sufficiently the freedom of expression interests at play. At the same time, there are legitimate concerns regarding how the Internet preserves and presents information about peoples' pasts. Decisions on this basis about whether to remove content require a delicate balancing that should ideally be done by expert, public decision-makers, not private search engines.

However, having been given this responsibility, search engines should develop detailed policies and standards regarding how they apply the right to be forgotten which ensure a proper balancing of the competing interests at stake. They should also consult with key stakeholders when developing these policies and standards. In terms of procedures, search engines should respect due process rights when applying the right to be forgotten ruling, including by informing those whose content is subject to a removal request, as far as this is legally permitted, and 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. Search engines should also implement their responsibilities in this area as transparently as possible, including by publishing detailed information about the policies, standards and decision-making processes they use to assess removal requests, as well as aggregated information about the number of requests received and how they were processed.

Transparency and Informed Consent

The Internet has fundamentally changed our relationship with information, which has, among other things, resulted in a rapid expansion of recognition of the right to information and a growing consumer demand for openness on the part of intermediaries. Where users' personal information is being stored and processed, there is also a broadly recognised right to track how this is being done.[22]

It has now become relatively common among major tech firms to publish transparency reports. Although the specific information provided varies, the central aim 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 underlying basis 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

[21] 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.

[22] 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.

the location of the requester and the uploader, and statistics about the final decisions on requests. 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 should publish information 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. Where legally permitted, companies should publish similarly detailed information regarding the nature and processing of requests by governments for user information. And where undue legal restrictions apply, they should be challenged whenever this is possible and reasonable.

Although it has become a common joke that nobody reads a company's terms of service, this lack of attention is troubling given that these terms serve as the legal basis for the relationship between the company and its users. The lack of public understanding of this legal relationship has important implications in terms of the core dynamic whereby users trade their privacy for services. For example, the fact that users so rarely pay attention to terms of service gives companies a licence to draft these terms incredibly broadly and/or vaguely or even, in some cases, in a deliberately misleading manner. This has resulted in a situation where, in many cases, it is difficult for even a careful reader to deduce the practical implications of terms of service.

This is not to minimise the legitimate challenges that intermediaries face in engaging users on these issues. Although various strategies have been employed, such as requiring users to scroll through to the end of the document before they can accept the terms, they 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.

Intermediaries should take steps to ensure that their terms of service and other polices are clear to users, including by publishing these terms of service in every language in which they offer services and by posting the information prominently on their websites. They should also support initiatives aimed at enhancing user understanding of intermediaries' policies.

Consultation is also important and intermediaries should consult with users prior to major amendments to their terms of service, notify users of any amendments they do make and make previous versions available online so that users can assess 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 part of the UN's Protect, Respect and Remedy framework,[23] 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. 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.[24] Although China is the most high profile example, companies face similar dilemmas in other countries, including developed democracies.

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. 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.

Avoiding complicity in human rights abuses should begin with undertaking a human rights impact assessment before a new market is entered or a new product is launched. 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.

Other measures to avoid complicity 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. Most global tech companies only maintain a physical presence in a few countries. 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 very real commercial implications this has. However, 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 (China may represent an exception here). 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

[23] 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.
[24] 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.

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, 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. 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.