Stand Up For Digital Rights: Recommendations for Responsible Tech[1]

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.

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

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 cut off access or deny service to a user unless required to do so by a clear and binding legal order.

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.

Recommendations for Content Moderation

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.

Recommendations for Protecting Privacy

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.

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, and their general approach to inter-jurisdictional reporting.
- 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.

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.