UNESCO's Comprehensive Study on Internet Related Issues

Submitted by :

Name: Emma Llanso

Gender: Female

Category of Stakeholder: A. civil society and NGOs including individual users

Country: United States of America

Region: Europe and North America

1. **What can be done to reinforce the right to seek and receive information in the online environment?**

Please see attached document.

http://unesco-ci.org/cmscore/sites/default/files/webform/internet-issues/question_one_unesco_survey_-_cdt_response.pdf

2. **What mechanisms can develop policies and common standards for open-licensed educational resources and scientific repositories, and for the long-term preservation of digital heritage?**

3. **How can greater progress be made as regards inclusive strategies for women and girls as well as marginalized and disabled people?**

4. **How can accessibility be facilitated through increases in locally produced and relevant content in different languages?**

5. **What can be done to institutionalize Media and Information Literacy (MIL) effectively in national educational systems?**

6. **What are the current and emerging challenges relevant to freedom of expression online?**

Social media and other platforms for user-generated content in particular have become vital fora for all manner of expression, from the private and personal, to the global and political. CDT believes that how we apply free expression principles to today's communications technologies

and beyond will determine the extent of freedom of expression enjoyed by the next five billion users who will join the global online community. [1]

Increasingly, the challenges confronting the right to seek and receive information online are also relevant to the right to impart information. In the era of "Web 2.0," online entities provide freely accessible platforms for the creation and dissemination of "user-generated content." On social media platforms, the expressive acts of seeking, receiving, and imparting opinion and information converge, and any meaningful distinction between speaker and audience begins to break down.

A. Limits on access to information also limit freedom of expression.

Censorship impairs the fundamental rights of communicators seeking to impart information and opinion to an audience, as well as the rights of audience members to receive their message—and, as user-generated content platforms proliferate—the audience's right to respond. Private takedown regimes and traffic management rules are also relevant to the freedom to impart information as to the right to seek and receive it. (See Question 11 below discussing the need for greater transparency from companies regarding their content policies and moderation/takedown practices.)

B. Malicious takedown attacks and user self-censorship present unique threats to free expression.

Defending networks from malicious exploits is increasingly important to preserve the freedom of expression of unpopular or controversial speakers. [2] Network attacks such as Distributed Denial of Service (DDoS) attacks have been used in recent years by private actors to overwhelm web sites with traffic, knocking them offline. [3]

Online association and expression are also highly susceptible to the chilling effects of the above-mentioned threats. The fear of exposure, intimidation, and violence in retaliation for the things one has written, watched, or read online can cause users to limit their online expressive activities. Speakers targeted for their statements become examples for other would-be speakers, who choose instead to censor their words. Repressive governments rely on Internet surveillance technologies to target political dissidents and human rights advocates for abuse.[ ] Similarly, intrusive monitoring, even for legitimate purposes, can have profound chilling effects on free speech. The risk of attack—through DDoS methods or in the physical sense—causes untold numbers of potential speakers to refrain from participating in online conversations.

Already, governments' use of certain invasive surveillance techniques that undermine Internet security may increase users' exposure to network attacks by malicious hackers, identity thieves, and foreign governments. [4] [5] [6] This increased vulnerability may cause many users to limit their online activities, including their speech.

[1] https://cdt.org/blog/freedom-of-expression-for-the-next-5-billion-internet-users/

[2] https://cdt.org/blog/it-takes-a-village-to-defend-a-network/

[3] https://www.cdt.org/files/security/000229judiciary.shtml

[4] https://cdt.org/blog/new-sanctions-combat-tech-mediated-human-rights-abuses/

[5] https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/

[6] https://cdt.org/blog/our-comments-on-nists-cryptographic-standards-review-process/

[7] https://cdt.org/blog/five-us-surveillance-programs-undermining-global-human-rights/

7. **How can legislation in a diverse range of fields which impacts on the Internet respect freedom of expression in line with international standards?**

CDT has addressed the necessary components of frameworks for Internet regulation that comport with international guarantees of free expression in a report entitled: “Regardless of Frontiers: The International Right to Freedom of Expression in the Digital Age" (attached). This report explores how the right to freedom of expression should apply in the Internet context. Specifically, the report examines new challenges (and opportunities) for freedom of expression in the digital age, including filtering, defamation laws online, jurisdictional issues, intermediary responsibility, anonymity, and Internet neutrality.

http://unesco-ci.org/cmscore/sites/default/files/webform/internet-issues/cdt-regardless_of_frontiers_v0.5.pdf

8. **Is there a need for specific protections for freedom of expression for the Internet?**

9. **To what extent do laws protect digitally interfaced journalism and journalistic sources?**

10. **What are the optimum ways to deal with online hate speech? How can Media and Information Literacy empower users to understand and exercise freedom of expression on the Internet?**

11. **What are the optimum systems for independent self-regulation by journalistic actors and intermediaries in cyberspace?**

In previous writing, CDT has explored the dilemmas, principles, strategies, and tools that content hosts and online platforms can adopt to mitigate the negative effects of content-moderation policies that include account deactivation or content removal. [1] [2] Hosts and intermediaries that support online speech should develop fair, consistent, and transparent content-moderation policies that provide their users with a clear understanding of the operator’s practices.

[1] https://cdt.org/insight/account-deactivation-and-content-removal-guiding-principles-and-practices-for-companies-and-users/

[2] https://cdt.org/blog/gni-report-shows-internet-companies-are-institutionalizing-privacy-and-free-expression-principles/

12. What principles should ensure respect for the right to privacy?

Privacy in the digital age requires the assurance of a number of other essential features of data protection, including the ability to choose whether to disclose or withhold our identity information and other sensitive data; transparency in data practices; and recourse for data breaches and other wrongful uses. These principles must be pursued while respecting other fundamental rights, including the right to free expression.

The ability to speak anonymously encourages individuals to freely use public and private communications platforms without fear that their identity will be revealed. As addressed in the response to Question 13, a right to exercise anonymity is essential for Internet users to be able to engage in a full digital life. Autonomy over the decision to withhold or disclose our identity information is essential for the free exchange of personal correspondence, sensitive or intimate association, and other legitimate online activities and transactions for which an individual may not wish to be identified. [1] The choice to exercise anonymity also allows speakers to openly express controversial beliefs, or to communicate with controversial people, without fear of retribution. [2]

Any legal or technical limits on anonymity must be transparently disclosed to users to inform their choices about whether to use a particular service or engage in a particular discussion on an online forum. [3] As addressed in Question 14, transparency about electronic surveillance and government access to user data allows individuals to make educated decisions about when to share their information, and fosters informed public debate on whether government surveillance programs adequately respect the right to privacy.

As addressed in Question 15, transparency is also a crucial component of protecting user data from misuse. Greater transparency in data use and maintenance practices would encourage businesses and governments to report theft or loss of identity and other sensitive information. These issues are especially salient as “big data” applications increase demand for personally identifiable information and increase the risk of data breach, as discussed in Questions 16 and 17. Users have a right to expect that information they entrust with data collectors will not be used against them, by parties with or without authorization to access their data.

As addressed in Question 19, media literacy is essential if users are to exercise rights over their identity and other personal information.

Finally, fundamental rights to privacy, transparency, free expression, and access to information can – and indeed, must – be reconciled as interacting and mutually reinforcing rights. CDT believes that workable legislation regarding digital privacy and transparency will also safeguard

essential rights to individual free expression, access to information, and democratic accountability, with due respect accorded to the personal preferences and dignity of users.

CDT feels that the proper balance between the public interest in privacy and in innovation lies in effective mechanisms for consumer control and notice of collection and use of data. CDT supports consumer privacy legislation that increases oversight, gives consumers access to databases compiled about them, and provides for redress in order to avoid possible discriminatory applications or other types of tracking and classification that conflict with shared values of privacy and equality.

[1] https://cdt.org/blog/contrary-to-rhetoric-study-shows-teens-benefit-from-use-of-pseudonyms/

[2] https://cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf

[3] https://cdt.org/blog/the-false-promise-of-anonymity/

13. What is the relationship between privacy, anonymity and encryption?

While related, anonymity and privacy are different concepts and present different technical challenges. “Anonymity” is the more clearly defined term of the two, representing the idea that an anonymous individual’s identity is completely separated from her actions and communications. (This is also different from a related term, confidentiality, where the individual’s identity is known but the communication is made secretly, in confidence.)

The option to remain anonymous is essential to engaging in sensitive correspondence, intimate associations, political speech, and legitimate activities and transactions for which an individual does not wish to be identified. Because of its importance to expression—both private and public—anonymity enables and enhances a range of fundamental freedoms, including the freedom of speech, freedoms of political association and religious affiliation, the right of access to information, and the freedoms of thought and belief. Technical anonymity is the practice of formally separating identity from activity and data, and there are tools that enable this (like the online anonymity software, Tor). However, there are limits to what technical solutions can accomplish: for example, if an individual identifies themselves in communications they make, or provides sufficient identifying details, there is little a technical system can do short of ceasing the conversation. This is to say, in the digital age, the practice of anonymity requires not only technical tools but also best practices that individuals must follow to protect their identities in these interactions.

Privacy is a less concrete concept both technically and philosophically. Privacy rules must empower individuals to make informed choices about how companies and governments collect, use, share, and maintain their personal information. For many advocates, privacy is defined as the ability to retain control over how information about you is collected and used. This implicates a number of other principles, including transparency and accountability, on which this definition relies. This articulation of privacy also depends on the ability to protect personal information from attackers trying to pry into otherwise private communications and data, which is less a philosophical problem and more one of practical security. In that case, protecting an individual’s

privacy means considering threats from the government as well as the results of commercial data collection and tracking. Privacy in one's identity allows speakers to express controversial beliefs, or to communicate with controversial people, without the fear of retribution.

Cryptographic technologies are what technical designers and developers use to protect the principles of privacy and security goals online. Cryptography is the current gold-standard of technical processes used in a practical manner to maintain privacy online. Current Internet and web services are capable of recording virtually every activity of users, including the information they receive and the people they communicate with. Tools such as encryption software and other secure communications tools are necessary for the secure transfer of personally identifiable information including credit card numbers, allowing anonymous Google searches, website visits, newspaper subscriptions, and purchases from online stores such as Amazon.com. Access controls, encrypted databases, and secure network connections make up the infrastructure for e-commerce and social life online. As a basic piece of infrastructure, these tools and techniques must be strong, without backdoors or engineered flaws.

The relationship between privacy, anonymity, and encryption is that each relies on a baseline of technical ability and personal control. When combined with technologies such as Tor, encryption can provide users with strong anonymity and privacy guarantees.

14. What is the importance of transparency around limitations of privacy?

Amid the contentious global debates about privacy and surveillance since the Snowden revelations, few proposed reforms have attracted more consensus than calls for greater transparency. The progress towards greater reporting on national security requests in the US demonstrates there is more that both governments and companies can say about surveillance demands without endangering national security.

Transparency is a necessary first step in supporting an informed public debate on whether domestic laws related to electronic surveillance and government access to user data adequately protect individuals' rights to privacy and freedom of expression. Transparency is also a crucial component for staving off abuses of surveillance and monitoring powers and content or account takedown regimes. The combination of government and company reporting can help the public understand the scope of restrictions on rights and dispel myths about surveillance or content removal.

Governments should make publicly available the laws and legal interpretations authorizing electronic surveillance or content removal, as well as report the aggregate numbers of requests, and the number of users impacted by these requests. Some governments have started to signal a willingness to make improvements on transparency. For example, the Freedom Online Coalition, a partnership of 24 governments working to advance online freedoms in their own countries and around the world, committed in April 2014 to promoting transparency and independent, effective domestic oversight over domestic surveillance programs. [1] But it is essential that these and other governments move toward specific reforms to ensure that they are meeting their transparency obligations.

Companies have also taken steps to be more transparent with their users about the requests they receive from governments. Since the Snowden revelations, US companies have filed legal challenges and supported legislation seeking the right to report about the national security requests they receive, and scores of companies have begun publishing transparency reports on government requests for user data. Internationally, telecommunications companies such as Vodafone have also begun to disclose this information, or to be transparent about where they are legally prohibited from reporting. [2] [3] [4]

Significantly more work remains to be done to achieve the level of transparency necessary to support an informed public debate about government surveillance and censorship practices. Working with other stakeholders, CDT and the Global Network Initiative (GNI) have developed a preliminary set of specific, actionable criteria for transparency, to help drive policy conversations toward implementable reforms. [5]

[1] https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf

[2] https://cdt.org/press/cdt-applauds-new-transparency-from-microsoft-and-facebook-as-important-step-calls-for-more-data/

[3] https://cdt.org/press/verizon-transparency-report-sets-industry-standard/

[4] https://cdt.org/press/linkedin-enters-the-surveillance-transparency-fray-in-a-big-way/

[5] https://cdt.org/blog/getting-specific-about-transparency-privacy-and-free-expression-online/

15. What kinds of arrangements can help to safeguard the exercise of privacy in relation to other rights?

Technical solutions can significantly enhance individuals' control over their identity and other personal information. Many companies now protect user information by default. [1] For example, Google recently released software that can be used to encrypt email, hiding the contents of emails from even its own automated scanning software used to display ads. In addition, Google is encrypting all bulk data transfers between its data centers, and it has added to its transparency reports a description of what email services are not allowing encrypted transfers of email. Facebook, Twitter, and other companies now encrypt their web pages by default, using particularly strong forms of encryption that change every time you make a new connection, thwarting some efforts at mass surveillance.

CDT applauds technology companies' recent steps towards a universally secure Internet through the adoption of ubiquitous encryption. [2] Techniques that rely on principles other than encryption, such as RAPPOR and randomization, may prove to be essential for preserving anonymity in the increasingly tracked world of targeted advertisement and big data.

There are exciting, emerging research results in privacy-preserving analytics that we believe could be bolstered and further incented by strategic research investment. There is already an emerging trend of developing and supporting end-to-end privacy solutions (where the keying

material is held only by the client) and usable privacy tools. These trends suggest that users are eager to find ways to control the collection and use of data about them and that companies are eager to design products to respond to that market. CDT supports efforts to increase transparency and privacy by continuing to develop technological solutions with privacy-enabling defaults and using elements of privacy engineering to ensure that privacy is deeply embedded in the design, rather than being reverse-engineered into a product or service. [3]

[1] https://cdt.org/blog/help-reset-the-internet/

[2] https://cdt.org/blog/polaris-lets-encrypt-will-mean-more-ubiquitous-web-encryption-and-privacy/

[3] https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/10/NSF-National-Privacy-Research-Strategy-Comments-Oct-17.pdf

16. How can openness and transparency of data be reconciled with privacy?

Transparency is an essential obligation on all governments. Governments are responsible for ensuring that the public understands the essential aspects of when and how surveillance programs operate, as well as any Internet content removal regimes, including notice-and-takedown regimes and the de-listing of search engine results. [1]

In the current debate around the implementation of the CJEU opinion in the Google Spain case, some have argued that individuals' privacy interests preclude transparency about link deletion demands. But de-listing search results that point to true, lawfully posted information that is part of the public record necessarily interferes with both the original author's right to impart information and the public's right to receive it. As with any government-imposed limitation on freedom of expression, this interference must occur only in a way that is predictable and transparent to all.

Governments and companies can reveal more about de-listing and takedown requests without compromising the individual privacy interests at stake. Governments must provide, and should allow companies to provide, clear reporting about the ways in which individuals' link-removal requests are affecting the information available for journalists, academics, researchers, artists, and other members of the public. Governments should make publicly available the laws and legal interpretations authorizing privacy-related removal requests, as should permit reporting of the aggregate numbers of requests and the percentage of requests that were granted, the frequency of various justifications for removal requests, and the number of users impacted by the requests. Transparency is a critical component to holding content intermediaries accountable, and ensuring that their implementation of their legal obligations is not biased, overbroad, or otherwise misapplied.

[1] https://cdt.org/blog/human-rights-and-surveillance-governments-must-comply-with-their-transparency-obligations/

17. What may be the impact of issues relating to big data on respect for privacy?

As innovative technologies emerge with new, sophisticated data collection capabilities, protecting users' privacy and ensuring data security has become increasingly important. Users share a wealth of sensitive personal information with companies that they rely upon for services. However, providing some information to a service provider should not imply that a user no longer possesses a privacy interest in her data.

Laws protecting against information abuse by "big data" firms could significantly improve individuals' confidence in speaking their minds and interacting online. [1] However, it is not clear how this data should be regulated. Traditionally, regulators have relied on accountability and transparency to give users control and access. But in the world of big data this is often impractical. Information is manipulated by algorithms that adapt as they digest and analyze more information and the specific mechanism by which a piece of information was categorized a certain way is often not obvious (even to the author of the program). The implications for privacy in big data often come down to questions of whether anonymization is feasible and whether it is reasonable to expect that a company can de-aggregate a data set to remove an individual's inputs if they ask. The legal and technical implications of a world of big data and machine learning are still being sorted.

In addition, the revelation that commercial data is tied to government surveillance has fundamentally changed the conversation about "big data." For the vast majority of consumers, unwanted surveillance—quite apart from practical effects of such surveillance—is itself a harm they wish to avoid. Any considerations of risks associated with "big data" must address harms from government surveillance as well as private sector risks. [2]

[1] https://cdt.org/blog/cdt-files-comments-in-white-house-big-data-review/

[2] https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/08/CDT-NTIA-Big-Data-FINAL.pdf

18. How can security of personal data be enhanced?

Users have a right to expect that information they entrust with data collectors will remain secure. The Fair Information Practice Principles (FIPPs)[1] generally track user expectations regarding the collection and safekeeping of sensitive information such as home addresses and credit card numbers, and personally identifiable information, including location data, browser history, and Social Security numbers or other unique identifiers. For instance, under the FIPPs, data collectors must be transparent about their collection and use of sensitive information (making information available about privacy practices) and they must give users adequate notice (providing contextual information about privacy practices).

Companies implementing the FIPPs must protect sensitive databases through the use of encryption, and should de-identify personal information wherever possible in order to minimize the impact of a data breach.[2] [3] Data collectors must also control access to the data, train employees, conduct oversight into business associates and partners who might also handle the data, and effectively manage encryption keys.

CDT has identified a number of ways in which industry self-regulation and government regulation can help to keep sensitive personal data secure.[4] It should be noted that any legislative security standard should offer the legal flexibility to evolve with future technological advancements. Therefore, CDT would recommend the use of a “reasonableness” security standard as opposed to specific technical security mandates.

[1] https://cdt.org/insight/protecting-consumer-privacy-in-an-era-of-rapid-change-a-proposed-framework-for-businesses-and-policymakers/

[2] https://cdt.org/blog/hhs-should-require-the-encryption-of-portable-devices-to-curb-health-data-breaches/

[3] https://cdt.org/insight/security-and-privacy-issues-associated-with-federal-rfid-enabled-documents/

[4] https://cdt.org/blog/cdt-weighs-in-on-ftc-privacy-report-protecting-consumers-in-digital-age/

19. How can Media and Information Literacy be developed to assist individuals to protect their privacy?

One of the most effective ways for individuals to protect their privacy online is by learning how to navigate the Internet safely. All Internet users should be able to provide for their own “digital hygiene” and for the basic digital security of others who have entrusted them with their sensitive information. There are measures everyone who operates a web page can take to make the Internet more secure, and there are simple steps that everyone can take to strengthen his own digital hygiene. [1] [2]

CDT has advocated for the development of “media literacy” programs and educational criteria to foster stronger personal privacy and security practices, particularly among young Internet users. Significant gains in media literacy may be achieved by integrating the use of the Internet and emerging technologies into school curricula, from pre-Kindergarten onwards. [3] The use of education and parental empowerment tools remain the best way for parents to create a safe online environment for their children.

CDT believes that a combination of media literacy and technical improvements that embed users’ intuition about privacy and security will be necessary for protecting privacy and the freedom of expression going forward. [4] CDT also supports Access’ “Encrypt All The Things” effort, which calls on Internet platforms to implement a seven step Digital Security Action Plan to safeguard individual data. User education on digital hygiene is one component of this holistic effort. [5]

[1] https://cdt.org/blog/help-reset-the-internet/

[2] https://cdt.org/insight/protecting-mobile-privacy-your-smartphones-tablets-cell-phone-and-your-privacy/

[3] https://cdt.org/blog/keeping-kids-safe-online-report-highlights-usual-suspects-education-parental-empowerment/

[4] https://www.cdt.org/files/pdfs/20091221_ftc_comments_privacy_design.pdf

[5] https://encryptallthethings.net/

20. **How can ethical principles based on international human rights advance accessibility, openness, and multi-stakeholder participation on the Internet?**

21. **What conceptual frameworks or processes of inquiry could serve to analyse, assess, and thereby inform the choices that confront stakeholders in the new social uses and applications of information and knowledge?**

22. **How does ethical consideration relate to gender dimensions of the Internet?**

23. **How can ethics, - i.e. the simultaneous affirmation of human rights, peace, equity, and justice - inform law and regulation about the Internet?**

24. **What international, regional and national frameworks, normative guidelines and accountability mechanisms exist of relevance to one or more fields of the study?**

25. **How do cross-jurisdictional issues operate with regard to freedom of expression and privacy?**

26. **What are the intersections between the fields of study: for example, between access and freedom of expression; ethics and privacy; privacy and freedom of expression; and between all four elements?**

27. **What pertinent information materials exist that cut across or which are relevant to the four fields of the study?**

28. **What might be the options for role of UNESCO within the wider UN system in regard to the distinct issues of online Access to information and knowledge, Freedom of Expression, Privacy and Ethical dimensions of the information society?**

29. **What might be options for the role of UNESCO in relation to stakeholders outside the UN system?**

30. **For each study field, what specific options might UNESCO Member States consider?**