University of California, Irvine
School of Law

Summary of Multi-Stakeholder Consultations in Preparation of the Special Rapporteur's Report on Freedom of Expression, States and the Private Sector in the Digital Age (A/HRC/32/38)

by UCI Law International Justice Clinic

Table of **Contents**

Front page image: "Internet of Things" by Dometorres
Source: Wikimedia Commons

I. Introduction

1. On December 3, 2015, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression **announced the launch** of a long-term project to explore issues at the intersection of State regulation of the Information and Communications Technology (ICT) sector, corporate responsibility, and freedom of expression. During the course of the project, the Special Rapporteur expects to hold a series of consultations with States, civil society, corporate actors, the technical community, academics and other relevant stakeholders.
2. The first consultation for the project primarily involved representatives from civil society, and was held on January 25-26, 2016, at the University of California Irvine (UCI) School of Law. A second convening bringing together corporate and civil society actors was held on February 29, 2016, at the Office of the High Commissioner of Human Rights (OHCHR) in Geneva, Switzerland. Both consultations were organized with the support of Article 19, OHCHR, and the UCI School of Law's Center of Globalization, Law and Society.
3. Both consultations were conducted under the **Chatham House Rule**.
4. Twenty participants (excluding the Special Rapporteur and his staff) attended the first consultation in Irvine, principally from civil society. Twenty-one participants (excluding the Special Rapporteur and his staff) attended the second consultation in Geneva, from both the corporate sector, civil society and international organizations. Participants came from all regions.
5. This report was compiled by students in the UCI School of Law International Justice Clinic and written by Amos Toh, Legal Advisor to the Special Rapporteur.
6. The report reflects points raised during the consultations ***but does not necessarily reflect the views of the Special Rapporteur or all participants*.**

II. Summary of Jan 25 – 26 Consultation

7. In the digital age, expression is increasingly mediated through private actors. This raises a host of questions about the scope and nature of the human rights obligations and responsibilities of the ICT sector, particularly with respect to freedom of expression (FOE).

8. Under the UN **Guiding Principles on Business and Human Rights**, the primary duty to protect human rights lies with States, which are required to create an environment conducive to business respect for human rights. Accordingly, the Special Rapporteur will also address FOE concerns raised by State regulation and action that affects the ICT sector.

9. At the start of the consultation, participants were asked to brainstorm a list of actors and stakeholders in the ICT sector for future study and analysis. Some of the lesser-known actors that were identified include: standard-making bodies; intellectual property (IP) rights holders; hardware companies and device manufacturers; network equipment vendors; domain name registrars; payment assistance platforms; software companies; data storage providers; and surveillance and cybersecurity companies.

Legal and Policy Issues

10. Participants subsequently identified a range of legal and policy issues as worthy of further research and advocacy:

11. Content Regulation

    a. Whether wittingly or not, there is a tendency among States to craft vaguely formulated laws and regulations that incentivize censorship. Just as concerning is State reliance on extralegal measures to monitor and censor Internet content. For example, there is growing pressure on Internet companies to proactively monitor lawful content that States nevertheless find problematic, particularly terrorism- and extremism related content. State mechanisms are also increasingly flagging lawful content on private developed content flagging mechanisms.

    b. Private policies and practices, including initiatives designed to regulate content, also implicate FOE, but the effects of these are generally less well-known and scrutinized. Issues of concern include: price

discrimination and 'zero rated' services; real-name identification requirements; restrictions on movement of expressive content between competing platforms; algorithmic manipulation to monitor or flag unsavory or controversial content; the impact of business relationships between Internet companies and content providers on content display; gaps, inconsistencies and unresolved tensions in company policies on online harassment, stalking and bullying; and accessibility of services for non-English speaking users.

c. There is an urgent need to synthesize high-level principles into pragmatic and situation- or sector-specific guidance on how companies should address censorship requests and other content regulation issues. As a general matter, ICT companies appear to be less equipped to handle these issues than privacy concerns.

12. Jurisdiction and Intermediary Liability

a. The nature of the Internet raises complex jurisdictional questions concerning the enforcement of restrictions on online expression. A single request for content takedown and access to customer data may have international effects beyond the territory of the requesting State.

b. Increasingly, States and private litigants look to hold private platforms and entities accountable for the actions of individual users that lie outside their jurisdictional reach. Debate about the appropriate scope of a company's liability for individual user actions is ongoing, and concerns about the chilling effect of overbroad intermediary liability on FOE are mounting.

13. The Right to Privacy and FOE

a. Excessive surveillance and other privacy-infringing measures have a significant and often directly adverse impact on FOE, and should remain a focus of the mandate.

b. Mass government surveillance of private digital networks, along with government access to customer data and laws requiring companies to modify or interfere with their software and equipment, continue to be urgent human rights concerns. In addition, the following issues at the intersection of privacy and FOE bear closer scrutiny: the right to be forgotten; Mutual Legal Assistance Treaties (MLATs); data localization; the policies and practices of network equipment and telecommunications infrastructure vendors; the sale of surveillance and cybersecurity equipment and technologies; and data mining for advertising and other commercial purposes.

c. On many of these issues, the lack of accountability is commensurate with the lack of proper documentation of State practice, and company policies and practices.

d. On the *right to be forgotten*, participants found that the current discourse is dominated by data protection principles, and sorely in need of FOE perspectives. There is significant uncertainty about how this right should be formulated and applied in a manner that is consistent with FOE.

e. On *MLATs*, participants observed that the current process is fraught with delay, lacks transparency and in need of major reform.

f. On the *sale of surveillance and cybersecurity technologies*, there is ongoing debate about the appropriate standard of human rights due diligence.

g. In general, it is important for companies to establish business practices that are sensitive to the diverse expressive interests of their users, particularly minorities. At the same time, too much knowledge about their users may pose risks to their privacy.

14. Transparency

a. States are under a human rights obligation to be transparent about their laws, policies and practices, both online and offline. States are increasingly passing laws that make it difficult for ICT companies to be transparent about actions that affect users' rights. The lack of transparency concerning trade negotiations that affect Internet freedom (including but not limited to the Trans-Pacific Partnership) is also concerning.

b. Most would agree that companies should be robustly transparent about their policies and practices. However, the harder question is: What statistics, indicators and categories of information should be disclosed – and how should it be disclosed and contextualized – to ensure meaningful transparency?

c. More or better transparency is required to illuminate, among other things, network and traffic management practices; the interpretation and enforcement of Terms of Service (TOS) and community standards; and the proportion of government-inspired actions vis-à-vis TOS-inspired actions; and policies and practices concerning the classification and arrangement of content.

d. Corporate transparency research and advocacy should also address private actors other than Internet intermediaries, including network infrastructure vendors, hardware and software companies, and surveillance and cybersecurity companies.

15. Due Process and Remedies

a. More research and study is required on the availability of effective remedies for FOE violations in the ICT sector, whether State-based or privately established.

b. In particular, the following questions were raised: What kinds of judicial and non-judicial remedies are required to vindicate FOE claims? What constitutes meaningful notice to a user subject to a content removal request, and are there opportunities to challenge those requests? How should privately developed complaints mechanisms address the concerns of non-English speaking users? How do considerations of scale affect the availability of remedies that sufficiently address the needs of large and diverse populations of users?

16. Responsible Entry and Exit

a. Considerations of market entry and exit vary depending on the type of platform or company in question. Internet companies do not have any real moment of entry given that their services are largely available as long as there is Internet connection; in contrast, Telcos and ISPs generally require permission to enter. However, this distinction may blur as State regulation and barriers to access become more pervasive.

b. On *market entry*, participants observed that the significant FOE interest in the products and services that many ICT companies provide might weigh in favor of entry. Assessments of responsible entry depend not only on *whether* companies enter, but also *how* they enter. For example, companies may exercise critical leverage to establish human rights safeguards when negotiating licensing agreements.

c. On *market exit*, participants debated the circumstances under which such a decision in the ICT context is a responsible action, if at all.

d. Participants observed that it is incumbent on companies to continuously identify and exercise leverage throughout their business relationship with States.

17. Human Rights Due Diligence

    a. Companies should take the initiative to make impact assessments a cornerstone of their business strategy. At the same time, it may be helpful for companies to conduct such assessments with the assistance of independent external experts, particularly in situations with multiple risks and competing considerations.

    b. Since many of the FOE implications of technology are emergent, assessments should be conducted regularly and flexibly to respond to changing circumstances.

    c. The degree to which due diligence processes should be transparent raises complex questions about the appropriate balance between the need for public accountability and the confidentiality required to conduct in-depth assessments of internal practices.

The Need for Diversity

18. Participants also discussed the need for the project to be diverse in scope. They emphasized the importance of meaningfully integrating developing world perspectives, particularly given the movement to characterize human rights and corporate responsibility standards as interferences with State sovereignty, as well as the concerns of marginalized and at-risk groups. The mandate should also pay special attention to the needs and concerns of local companies, which may be more vulnerable to FOE restrictions than multi-national corporations.

Desired Outcomes of the Project

19. Finally, participants discussed possibly desired outcomes of the project. The following goals were identified:

20. Principles and guidance: The mandate could develop guidance that operationalizes FOE standards and, where necessary and practicable, identifies 'red lines' that no State or company should cross. The mandate could prioritize guidance that addresses segments of the ICT sector that are under-scrutinized. Such guidance should be concise.

21. Thematic Reports: Civil society and the corporate sector have relied extensively on the mandate's thematic reports in their policy and legislative advocacy and litigation. Such reports should continue to address the issues identified above. Future reports should also articulate the precise legal and policy bases for the corporate responsibility to respect human rights in the ICT sector. Future reporting might benefit from case studies analyzing specific

cases where internal corporate human rights processes have effectively addressed FOE issues.

22. Government Engagement: The mandate should use country visits to direct the spotlight on State practices in the ICT sector that are concerning, particularly outside U.S. and Europe. The mandate should also develop guidance that reiterates and elaborates on States' obligations to protect and advance FOE in specific contexts is also helpful. The mandate should expand its consultations to include representation from State security agencies.

23. Multi-stakeholder engagement: The mandate should explore opportunities for collaboration with other relevant Special Procedures, regional mechanisms, and academia. Particularly in geographical hotspots, the mandate should exercise its convening power to facilitate dialogue between civil society and governments. The mandate should also facilitate the development of multi-stakeholder initiatives tailored to regional needs and concerns.

24. Corporate Engagement: The mandate should prioritize visits to ICT companies that are under-scrutinized and/or that civil society has difficulty engaging with, particularly in non-Western countries. Such visits should convey the importance of addressing the FOE implications of their businesses, institutionalizing FOE commitments, and engaging with non-industry stakeholders.

***

III. Summary of Feb 29 Consultation

Legal and Policy Issues

25. During the first half of the convening, participants were asked to identify legal and policy concerns within the ICT sector that implicate freedom of expression. Participants identified concerns in the following areas:

26. Content Regulation

    a. State regulation of Internet content may stem from a need to advance legitimate objectives, including copyright law, child protection, hate and offensive speech, and cybercrime and cybersecurity. However, the establishment and enforcement of content restrictions in pursuit of these objectives are often overbroad.

    b. Concerning trends in content regulation include: (1) Unwritten extralegal or -judicial measures to block or take down content that evade documentation and scrutiny; (2) the spread of the right to be forgotten post-*Delfi AS vs. Estonia*; (3) overbroad requests to Telecommunications companies (Telcos) and Internet Service Providers (ISPs) to block access to entire platforms and websites instead of specific webpages or videos; (4) lack of due process safeguards or transparency concerning the enforcement of content restrictions; and (5) vaguely formulated content restrictions (e.g. hate speech laws with no meaningful guidance on what constitutes "hate speech"); (6) overbroad interpretations of relatively well-defined content restrictions (e.g. censoring discussions of online gambling on social media platforms under a prohibition against online gambling ads); and (7) the growing criminalization of speech (both online and offline).

    c. A major reason for many of these trends is a lack of technical understanding of how the Internet works at all levels of government. Many States do not understand the technical limits on private content monitoring and blocking, and assume that filters that private platforms apply to child sex abuse images are readily transferrable to all other contexts, including restricting 'extremist' content. However, unlike the filtering of child sex abuse images with identifiable digital markers, other forms of content moderation require the exercise of human judgment and discretion. Legislatures are also often unaware that targeted alternatives to website blocking are available.

d. The prevalence of ad blocking was also identified as a form of privately developed content regulation that threatens expression on Internet platforms.

27. Shutdowns, Filtering and Throttling

a. Participants identified a need to investigate and document the frequency and economic costs of network filtering and website shutdowns, especially in areas where the Internet is critical to economic growth. However, shutdowns are particularly difficult to document because they are often shrouded in secrecy: It is rare to see a shut down authorized by judicial order. Additionally, Telcos and ISPs are frequently prohibited from disclosing requests for shutdowns, and may even be asked to mislead the public as to the cause of the interruption.

b. Recently, the throttling or slowdown of traffic to platforms and websites have also become censorship mechanisms of choice. Typically, States will request ISPs to slowdown traffic to and from a particular website or platform (e.g. 2 to 3% of normal bandwidth). Such incidents are also difficult to document for the reasons identified above.

c. Increasingly, State reliance on these censorship mechanisms is tactical and strategic: Websites containing relevant sensitive information and entire networks are more often than not blocked in anticipation of or during certain political or social events and anniversaries.

28. Intermediary Liability:

a. Many Intermediary liability regimes, like 'notice and takedown,' are set up in a way that co-opt internal corporate processes as the de facto alternative to legal process. These trends place social media, search engines and other Internet platforms – which are not inherently bodies of democratic governance – in a position to make decisions concerning legal/legitimate vs. illegal/illegitimate content.

b. There is a need to identify positive examples or aspects of intermediary liability regimes developed through domestic legislation.

29. Terms of Service (TOS)

a. At least two factors influence the formulation of TOS: Local law and corporate values. Companies are typically more beholden to content restrictions under local law if they have a local presence.

b. As to the question of whether TOS should be drafted in a manner consistent with human rights standards, several participants were of the view that Internet companies should be free to establish TOS that is consistent with the vision of the community they wish to create. Others asked whether this freedom should be qualified if the service or platform is a dominant player or exercises monopoly.

c. On the practice of States requesting takedowns through private content flagging mechanisms, several participants observed that companies may be unaware of the origin of such requests if they are submitted anonymously. However, companies treat such requests in the same way they treat those from private parties.

30. Surveillance and Digital Security

a. On *government access to customer data*, participants observed that companies are often forced to choose between the safety of its local employees and the need to protect the privacy of user data. Concerted pushback from the international community is required when governments make surveillance demands that go beyond the law.

b. On *covert surveillance*, there is still little transparency about whether and how governments obtain direct access to private networks and platforms despite the Snowden revelations.

c. On *user registration requirements*, participants were concerned that such requirements facilitate government surveillance. The failure of Telcos and ISPs to register users has led to hefty fines.

d. On *big data*, the potential government misuse is deeply concerning. While such data can be useful, safeguards against abuse must be developed.

e. On *the sale of network infrastructure*, there is a lack of clarity concerning the human rights standards applicable to the development and sale of interception capabilities. The prospect that governments are covertly introducing backdoors into network equipment is also concerning.

f. On *data localization*, such requirements are often justified on the basis of competitive equality and user privacy. In reality, they are designed to enable State access to customer data.

g. On *Multinational Legal Assistance Treaties*, the process is cumbersome and fraught with delay and inefficiency. Without reform, there is a

greater threat of data localization, and overbroad assertions of extraterritorial jurisdiction.

31. Transparency: States are generally not transparent (or transparent enough) about their content takedown requests (whether law-based or extralegal) and interpretations of content restrictions. At a minimum, takedown requests should be made in writing, include relevant information such as the reasons for removal and references to applicable law, and where possible, should be approved by a judge.

Corporate Responsibility and Strategies to Respect Freedom of Expression

32. Participants also discussed the scope and implementation of the corporate responsibility to respect freedom of expression. Among the strategies and issues discussed were:

33. Responsible Entry and Exit:

    a. Human rights impact assessments at the point of market entry are a critical measure of the risks and benefits of entry. Such assessments examine, among other things, the human rights impact of local laws and opportunities for human rights advancement in that jurisdiction.

    b. For many Internet companies, it is difficult to pinpoint a moment of entry: Their platforms are available globally unless steps are taken to block them. When such blocking occurs, however, due diligence processes might apply during negotiations with governments on conditions for local access to the platform or service. Such processes may also apply during product design and decisions concerning infrastructure investments.

    c. There is a lack of consensus on the circumstances under which Telcos and ISPs should exit a market (if at all). The risks of market exit include loss of technical infrastructure and other investments, and the entrance of alternative providers that are less human rights compliant. The obligation to exit responsibly is also complex and multi-layered, and might require external expertise.

34. Due Diligence:

    a. Human rights impact assessments and other due diligence processes are conducted for a wide variety of business decisions. The availability and quality of due diligence processes often depends on the state of human rights and development in the company's jurisdiction of origin. Compared to well-established companies, small and medium

enterprises are understandably preoccupied with raising venture capital and therefore less likely to assess the human rights impact of their business.

b. Educating senior management and business development teams on the importance of due diligence is critical. Due diligence is central to a company's business strategy because it not only protects human rights, but may also enhance user experience.

c. The actions ICT companies take to mitigate the human rights impact of their businesses may often take place behind closed doors, for a variety of commercial, legal, regulatory and strategic reasons. Mitigation strategies may include legal review, risk assessments, user notification, proportionality analysis and improvements to technical standards.

d. Intra-industry collaboration facilitates knowledge sharing about effective mitigation strategies, and builds leverage with governments. Civil society and media engagement are also critical to effective resistance against problematic requests and laws. Finally, relationship building with governments also creates opportunities for dialogue and negotiation.

Potential Strategies and Opportunities for Engagement

35. Finally, participants discussed the mandate's potential scope of engagement the issues identified above, and opportunities for research and advocacy, whether independently or in collaboration with the ICT sector. In particular, participants discussed the following tools and strategies:

36. Communications: The mandate regularly **communicates** with States regarding alleged FOE violations. While response rates vary among States, these communications create a public record of alleged FOE violations that may encourage meaningful government engagement. Companies should reach out to the SR if an issue or problem they encounter is ripe for a communication.

37. Practical Guidance: Practical guidance that translates high-level principles into best practices and situation-specific standards is required. Such guidance should be short, pithy and available in multiple languages. Examples and templates of content regulation and surveillance laws that are human rights compliant are required.

38. Documentation: It will be useful to create a repository of censorship incidents and analysis of content blocking patterns. A database of licensing agreements and requirements would also be helpful.

39. Corporate Visits: Visits to ICT companies with less human rights awareness are critical to improving understanding of why and how to respect FOE. Visits to companies with a higher degree of human rights awareness are also useful because they provide opportunities for confidential discussions of relevant sensitive information concerning business practices.

40. Regional Engagement: Meaningful collaboration with regional bodies and fora neutralizes the critique that the mandate's advocacy has Western bias. In particular, it is critical to develop human rights strategies sensitive to the needs, concerns and realities of operators and intermediaries headquartered or operating in the Global South. Engagement with governments in these areas is necessary.

***