International Law Programme
Meeting Summary

CHATHAM HOUSE
The Royal Institute of International Affairs

Challenges to Freedom of Expression

Sherif Elsayed-Ali

Head of Technology and Human Rights, Amnesty International

Professor David Kaye

UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

Chair: Sonya Sceats

Associate Fellow, International Law Programme, Chatham House

20 July 2016

10 St James's Square, London SW1Y 4LE T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
www.chathamhouse.org
Patron: Her Majesty The Queen Chairman: Stuart Popham QC Director: Dr Robin Niblett Charity Registration Number: 208223

Introduction

This summary provides an overview of a meeting convened by the International Law Programme at Chatham House on current global challenges for freedom of expression (FoE).[1] During the event, five key areas of consideration emerged:

1. The rationales driving restrictive government policy.
2. The diversity of tools used to curtail FoE by different governments.
3. The tension between countering violent extremism (CVE) and human rights.
4. The competing models of cyber governance and their sustainability.
5. Strategic, global responses to the challenges to FoE.

The meeting was held on the record with panellists speaking in a personal capacity.

Rationales driving restrictive government policy

Governments around the world have adopted increasingly restrictive policies with regard to FoE. As a consequence, the space for civil society and groups including women, LGBT community, and secular entities is shrinking. There are a number of rationales that are, to differing extents, driving these policies.

Countering violent extremism

With the threat of terrorism, CVE has come to dominate the global political agenda, resulting in restrictions of FoE. The Investigatory Powers Bill in the UK[2] and the surveillance law[3] passed in the wake of the January 2015 attacks on the offices of Charlie Hebdo in Paris are examples of CVE measures adopted by Western governments. Participants of this meeting were of the view that authoritarian states observe such polices in Western democracies and understand that CVE is a priority. Consequently, the West is more likely to turn a blind eye to states adopting measures that restrict FoE, apparently in the name of CVE. Tajikistan, for example, has adopted a number of restrictive measures despite never having had a serious issue with terrorism. Attendees asserted that these measures lack the detail and nuance of the legislation being imitated. The impact has been media blackouts and suspensions of communication networks. Additionally, with the justification of CVE, Tajikistan has restricted the media, civil society and political opposition.

Measures that seek to tackle violent extremism while respecting FoE were noted. A number of states, for example, have adopted measures seeking to educate and integrate immigrants. The Netherlands has a programme that seeks to identify individuals at risk of radicalization through a non-criminal framework. Guarded support was offered for such policies. The main difficulty identified was the lack of rigour that governments are able to apply when outsourcing CVE to non-government actors. Consequently, there can be great scope for error leading to the subsequent radicalization of those involved in such programmes.

[1] This summary was prepared by Alex Shellum.
[2] At the time of publication, this Bill had not yet received Royal Assent.
[3] Loi No. 2015-912 du 24 juillet 2015 relative au renseignement (1) [Law No. 2015-912 of 24 July 2015 Regarding Intelligence (1)], https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorie Lien=id.

Preservation of government control

The internet has decentralized and democratized access to information and to communication. As governments are instinctively centralized and the loss of control over the flow of public information is counter-intuitive, restrictive policies may reflect a desire reassert control over public information. The growth of the power of corporations within the digital sphere was also cited as a contributing factor. This rationale is employed by democratic and non-democratic countries alike, as exemplified by David Cameron's speech in the aftermath of the 2015 Charlie Hebdo attacks calling for full access to online communications.[4] It was questioned whether such policies were viable from a technological perspective.

Some governments pursue policies that restrict FoE in order to preserve the integrity and control of government. This rationale often lies beneath the public consciousness as CVE is cited as the primary rationale in open forums. The concern of these governments is that technology provides greater scope for the expression of opinion and possible democratization. The case study of Tajikistan was again cited as an example of this practice.

Protecting morals, religion and against offence

A further rationale driving restrictive government policy concerning FoE is the desire to protect traditional values, religion and against offence. Similarly, it has become commonplace in some states to enact laws specifically protecting government officials from insults and verbal abuse.

Tools used to curtail freedom of expression

Traditional censorship

Arrests and criminal proceedings are frequently used to restrict FoE. Broad definitions of terrorism have meant that human rights defenders, with no affiliation to terrorist organizations, are often labelled as threats to national security. In some African and Asian countries, individuals risk detention, investigation and litigation for criminal or civil defamation or sedition. Again, the Tajikistan case study proves illustrative; in recent years, a number of leading figures in the Islamic Renaissance Party of Tajikistan (IRPT) have been arrested and tried in secret under the guise of CVE.[5] Alarm was expressed that governments in some quarters, through acts or omissions, are increasingly relying on violence against these actors in order to limit FoE.

It was argued that governments often use the legal system to impose oppressive bureaucratic requirements and unjustified oversight to limit certain groups' capacity to operate and, as a consequence, their FoE. Social justice organizations, for example, are categorized as foreign agents and organizations, which discredits them and jeopardizes their financial and legal status. There are also increasing restrictions on foreign funding.

Technological censorship

Authoritarian governments have learned from the 2011 Tahrir Square protests in Egypt, during which social media was instrumental in the organization of public protests. Shutting down entire services and networks during times of unrest has since become routine. For example, Tajikistan's security services

[4] BBC News (2015), 'Can the government ban encryption?', 13 January 2015, http://www.bbc.co.uk/news/technology-30794953.
[5] Human Rights Watch (2016), 'Tajikistan: Severe Crackdown on Political Opposition', 27 February 2016, https://www.hrw.org/news/2016/02/17/tajikistan-severe-crackdown-political-opposition.

have argued that blanket shutdowns are necessary as they lack the technological capacity to filter specific websites and ideas. Participants expressed doubt as to the validity of this claim. The prevalence of this practice internationally was echoed by another participant who confirmed that there has been a significant increase in the shutting down of communications networks in states including Turkey, Ethiopia, Gambia and Iran.

Another tool for restricting FoE made possible by technology is mass surveillance. One participant noted that surveillance, or the perception of surveillance, is making work extremely difficult for civil society actors. Intrusive surveillance techniques are also a tool deployed by democratic governments. The danger for FoE and also privacy in these cases is that surveillance systems in democratic, wealthy countries are sophisticated and it is difficult to identify any intrusion. In particular, it was claimed that the British government had spied on Amnesty International's communications.[6]

It was noted that Article 19 of the International Covenant on Civil and Political Rights (ICCPR) allows governments to impose restrictions on FoE but only when such restrictions are provided for by law necessary, and proportionate, to the legitimate aim pursued.[7] The requirement that restrictions be provided by law demands not only that a codified law exists before a restriction is imposed, but also that the rule of law must be respected. It was stated that there is a role for the judiciary, as an independent entity, in authorizing targeted surveillance. One speaker claimed that an independent judiciary is essential in ensuring the appropriate restriction of FoE where necessary. For example, the ability of judges to serve as independent, legitimate monitors on government behaviour was cited as a key issue in the debate on the UK's Investigatory Powers Bill. Judicial oversight may be assuming increasing importance in this arena due to the inability of the public to stay abreast of complex technological developments and the lack of legislative scrutiny across states generally. This raised the question of whether the judiciary should be educated on the latest technological developments so as to serve the required scrutinizing function.

Prior censorship

Prior censorship is a tool frequently applied to the arts. The approval or disapproval of film scripts, for example, is a way in which expression is censored prior to the act. It was argued that this form of censorship is prohibited under the ICCPR and the Universal Declaration of Human Rights (UDHR). However, states may impose prior restraint on FoE on grounds of national security, and therefore states in military situations continue to use prior censorship. The broad view at the meeting was that the abuse of the prescribed exceptions to the ICCPR and UDHR presents a further challenge to FoE.

The tension between countering violent extremism and human rights

From a CVE perspective, the perceived need of governments to control the flow of information has never been greater. This has in turn been matched by an increased capacity to control the flow of information. Among human rights guarantees, FoE is notable in that its governing provisions in international human rights law (Article 19, UDHR, ICCPR) have inbuilt extraterritorial application. That is, they provide

[6] Amnesty International UK (2014), 'Why we're taking the UK government to court over mass spying', 14 July 2014, https://www.amnesty.org.uk/why-taking-government-court-mass-spying-gchq-nsa-tempora-prism-edward-snowden.

[7] Article 19(3) ICCPR reads:

> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.

everyone with the right to seek, receive and impart information of all kinds 'through any media' and 'regardless of frontiers'. There exists therefore a tension between the CVE agenda and human rights.

The problematic nature of mixed messaging from the UN was raised in this regard. The UN Special Rapporteur on Counterterrorism's report advised against criminalizing extreme but peaceful views.[8] This could be a means of relieving the tension between CVE and human rights. Such an easing of tension would be particularly beneficial in the academic context where there is a pressure, through policies like Prevent in the United Kingdom, for individuals to act as watchdogs on extremism. Where this happens, there is a greater risk of inhibiting expression.

Competing models of cyber governance and their sustainability

Presently, the prevailing model of cyber governance is the multi-stakeholder model. It is clear that governments are involved in cyber governance but only as one of a range of actors. Other actors include: those in the technical community who build the internet and the protocols that enable communication; civil society; academics; corporations responsible for building the infrastructure of the internet, such as Internet Service Providers (ISPs); and corporations responsible for building the platforms that users use to communicate, such as Facebook and Twitter. The rationale behind the multi-stakeholder approach is that it ensures that no one particular organization or group governs the internet. This has been essential to the internet's growth as it protects against both government and corporate control. The consensus in discussion was that the multi-stakeholder model is desirable.

The alternative to the multi-stakeholder model is the governmental model. China is the main proponent of the governmental model, although Russia and a number of other states are also in favour. The Chinese internet is one that is strictly controlled in terms of content and access by the government. There was disagreement among participants as to whether this significantly diminished the vibrancy of expression on the Chinese internet. Under the governmental model, regulation would take place at the level of the International Telecommunications Union (ITU), whereas at present regulation takes place in a number of forums globally.

The line between these models, however, is at risk of becoming blurred. The identification of the power of corporate actors in cyber governance has induced governments of all persuasions to seek to arrogate to themselves control over digital technology. One participant stated that Western governments, while wedded to the multi-stakeholder model, are increasingly turning to data localization in pursuit of this end. Data localization is a policy that requires that foreign companies store citizens' data in datacentres within the country of their nationality. This ensures that the physical infrastructure of the internet is in the possession of governments, thereby negating the adverse effect on governmental control that is characteristic of the borderless nature of digital technology. Data localization, therefore, renders digital technology far closer to a physical technology, such as nuclear technology, which is easier to control. The danger of the proliferation of data localization and similar technologies, according to one participant, is that it constitutes a shift in cyber governance towards a de facto governmental model.

The sustainability of current models of cyber governance

In response, it was noted that the contest between these two competing models will become a major long-term challenge for cyber governance and therefore also for FoE. At present, the West has been successful

[8] Human Rights Council (2016), 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', Ben Emmerson QC, 22 February 2016, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session31/Pages/ListReports.aspx (A/HRC/31/65).

in ensuring the vitality of the multi-stakeholder approach, and it is an issue about which Western governments feel strongly. Even so, one speaker predicted that this would become an area of real tension that could have a large impact on citizens globally, as it already does at the domestic level in China, Russia, and elsewhere.

However, doubt was expressed by another speaker as to the long-term viability of the governmental model as seen in China. The reason for this is connected to the problem for governments that data localization seeks to solve – the borderless nature of digital technology makes it difficult to control, which is the hallmark of the governmental model. Therefore, the nature of digital technology itself casts doubt on the sustainability of the governmental model of cyber governance in the long-term.

Uncertainty was expressed in response to how the pace of technological developments will impact upon each model's sustainability. At present, it is clear that the intersection between the public and corporate sectors has created a situation in which society willingly engages with the surveillance environment through the use of Google and social media. The arrangement, however, is fluid. The Edward Snowden revelations have caused the corporate sector to take a more robust approach to governments, which in turn has elicited a legislative response from governments globally on cyber security to address the issue of information collected online. The panellists agreed that such legislation is an attempt by governments to 'play catch up' in respect of digital control. The combination of the relative youth of the current models, the rapid pace of technological change, and the fluid relations between the public and corporate sectors, makes it difficult to assess the long-term sustainability of either model of cyber governance. It was suggested that a clearer picture is only likely to emerge over the next five to seven years.