Index Policy Note

Standing up to threats to digital freedom

Can we keep the internet free?

December 2012

The future of the internet is at stake as major governance decisions are made. The battle lines are being drawn between those who see freedom of expression as a fundamental human right in the digital world as much as it is offline, and those that consider the control of information and ideas as a priority for the state.

Freedom of expression – the freedom to send, receive, share and access information and ideas (in any media) – is a core right, vital to the exercise of most other rights; if it is compromised online it will undermine free expression and other rights offline as well as in the digital world. Yet we see a rapid increase in the number of governments – some authoritarian, but some democratic – stepping in to increase their control of the internet. We also see a number of corporations (web hosts, ISPs, telecom companies and others) sometimes working with governments when they engage in censorship, surveillance or other harmful interventions in the internet, and/or acting as increasingly powerful private actors determining the boundaries of our scope for free expression (as captured in the phrase 'the privatisation of censorship').

Internet Governance

The freedom, openness, growth and innovation of the internet are largely a result of its decentralised and open system of governance. As UN Special Rapporteur on freedom of opinion and expression Frank La Rue highlighted in his report last year, the internet enables individuals "to exercise their right to freedom of opinion and expression, but also a range of other human rights, and to promote the progress of society as a whole."

A number of states are now starting to challenge the decentralised, open governance of the internet and propose a more top-down system of control. Such top-down regulation would severely threaten freedom of expression, limiting sharply the openness and creativity that current structures allow: free speech and top-down control stand in opposition to each other.

To preserve the Internet's expanding global role in facilitating human development and democratic participation means preserving its future as a technology defined by freedom and innovation. This means resisting both public and private efforts to limit a proven policy and technical standards framework based on openness, competition, access and freedom of expression.

If the future governance of the internet were in the hands of a global regulatory body there is no doubt that certain countries would attempt to undermine the multiple underpinnings that ensure internet freedom. Russia and China have been vocal in their desire both to see a more top-down regulation of the net and for the US to lose some of the particular levers of control that it has. Yet it is clear that neither of them is a supporter of internet freedom or free expression. This month, Russia's planned blacklist of websites that promote drugs or suicide or contain porn or "extremist" materials came into effect, just one example of a trend to control, filter and block content and one that increasingly chills free expression. China, a country of 500 million internet

users, also finds ever more sophisticated ways of censoring the web and monitoring users -- from blocking IP addresses to filtering keywords and search terms.

The next *rendezvous* point for those pushing for top-down regulation is the December meeting of the World Conference on International Telecommunications (WCIT), organised by the International Telecommunication Union (ITU – a specialised UN agency that sets standards for international telephony). Leaked proposals have revealed how various governments seek to rewrite international telecommunications regulations (ITRs) to incorporate regulation and control of the internet. Such a move is strongly opposed by the US and EU but there is concern that a number of other key states including India, Brazil and South Africa, who have called for a global internet governance body within the UN, could support these ITU moves by Russia and China.

- **Establishing a global body exercising top-down control of the internet would risk increased censorship and suppression of free speech – not least given the number of countries and states already censoring and monitoring the net – and would be likely to severely erode openness and inhibit innovation and creativity.**
- **A multi-stakeholder, bottom-up structure of internet governance is a vital component of ensuring an open and free internet through which freedom of expression and other fundamental rights can be promoted and defended.**

State and Corporate Censorship

The number of countries and states censoring the internet and digital space in some way has increased substantially in recent years – from single figures to over 40 states today (according to the Open Net Initiative). While some of the worst cases are predictable, including China, Iran, North Korea and Saudi Arabia, much of the increase is in western countries including in the European Union. Traditional defenders of free speech in the EU, such as some of the Nordic countries, are among those introducing national level filters, while the UK's draft Communications Data Bill would set a deeply worrying precedent if it goes through, with its provisions to monitor the entire population (from email to mobile calls and website tracking). In Azerbaijan, more traditional offline repression tactics, including violence and imprisonment, are often used to intimidate and encourage self-censorship in the digital world.

Firewalls and Filters

Authoritarian states continue to be very active in online censorship, from China's Great Firewall to plans in Iran for a "halal internet" detached from the wider world. Meanwhile, the Russian government recently pushed through a bill that will allow websites classified as "extremist" (often a catch-all term in Russia) to be blacklisted without judicial oversight. The inappropriate, intrusive or excessive use of filters and firewalls is an increasing issue in democracies and transition states too, with a range of impacts on free expression, access to media, and on the nature of news provision. Sometimes these filters and firewalls are at the behest of governments but sometimes they are the initiative of private companies.

Intermediary Liability

Regulating intermediary responsibility is another way governments demand companies censor content. In April 2011, India's Ministry of Communications and Information Technology issued new guidelines for "intermediaries" (such as internet service providers), under which internet companies are expected to remove content that regulators deem "grossly harmful," "harassing," or "ethnically objectionable" within 36 hours. Failure to comply could land companies with fines or possible jail time. These guidelines blur the line between service provider and publisher and chill digital free expression.[1]

Takedown Requests

The excessive and inappropriate use of takedown requests by governments, and private individuals or companies can be highly chilling and impact on online debate, from social media to comment threads and more. There is a lack of adequate data to monitor the extent and source and motivation for takedown requests, although the transparency reports now issued both by Google and by Twitter start to show which governments are most active in issuing such requests, whether they are backed by court orders, and whether the company (Google or Twitter) complied – with the US making the most requests to Twitter in 2012 and India making the most to Google.

Privatisation of Censorship

Private companies – ISPs, web hosts and others – face the challenge of operating in a range of countries and at the same time ensuring they respect fundamental human rights. National laws and fundamental rights will sometimes be in conflict and companies need to be clear and transparent about their principles for operating in different states and on what basis they respond to government takedown requests. In October, Twitter announced it had blocked the account of a far-right German group, banning it in response to a government request based on Germany's strict anti-extremist legislation. While the primary responsibility for this example of censorship lies with Germany's laws, companies should not be direct participants in unwarranted censorship.

The Global Network Initiative (of which Index is a member) is one approach to bringing together companies and human rights groups to ensure basic principles and rights are respected in the digital world.

Private companies, such as Facebook, Twitter, Google and others, are also in many cases playing an increasing role in delineating the boundaries of 'acceptable' speech – and setting chilling rules on anonymity and real name use – through their own terms of service and codes. Some argue that terms of service can be seen in effect as editorial choices (or similar to a club having a set of rules) but, given the reach of large global players such as Google and Facebook, these companies are starting to regulate what is effectively public space in a way that would

[1] A study by the Bangalore-based Center for Internet and Society has shown that the 2011 rules "create uncertainty in the criteria and procedure for administering the takedown thereby inducing the intermediaries to err on the side of caution and over-comply with takedown notices in order to limit their liability and as a result suppress legitimate expressions."

previously have been the preserve only of states and governments. This opens up questions of the basis on which companies set their rules and codes and terms of service and how they can and should be challenged and held to account.

Criminalisation of Speech

Another aspect of state censorship is the growing trend in many countries to criminalise speech and free expression in response to the growth in digital communications. In October this year, the Bahrain Interior Ministry announced the arrest of four people for defaming public figures on social media. Also in October, Turkish pianist and composer Fazil Say was put on trial in Istanbul for insulting Islam in Twitter posts. And at the start of 2012, journalist Hamza Kashgari fled his native Saudi Arabia, where he faced the death penalty for tweeting a mock conversation between himself and the prophet Mohammed.

Criminalisation of speech on social media networks has also been increasing in the United Kingdom under the outdated Communications Act 2003. Most recently, a 20-year-old man was sentenced to 12 weeks in a young offenders' institution for making a sexually explicit joke on social networking site Facebook about a missing five-year-old girl. As the UK's Crown Prosecution Service prepares interim guidelines on social media prosecutions, there is an urgent need for an end to criminalising speech that is poor taste, or offensive to some, or simply a joke.

- **State and corporate censorship are increasingly threatening freedom of expression in the digital world. Neither states nor companies should be in the business of putting country or network-wide filters or firewalls in place with the aim of chilling or censoring free speech.**
- **Takedown requests should always be backed by a court order, and as with free speech offline any limits must be highly constrained and transparent.**
- **Intermediaries should not be made responsible for censoring content, and private companies should fully respect their human rights obligations in their operations around the world.**
- **Governments must not move in the direction of criminalising speech and digital communications in ways that will chill free expression and risk dampening the use and development of social media.**

Surveillance, Privacy and Free Expression

Respecting an individual's right to privacy goes hand in hand with respecting their right to freedom of expression. Yet the technological ease of gathering a large amount of information on individual citizens through monitoring their digital communications, for both commercial or repressive reasons, has led not only authoritarian but also some democratic governments to move in the direction of mass surveillance. At the same time, we are also seeing some private

companies going too far in invading users' privacy and both utilising and publishing data for commercial reasons. The right to privacy and the right to freedom of expression are closely linked: if individuals' communications are monitored, that will directly chill their free expression and encourage self-censorship.

In China, technological and human surveillance combine to create one of the most monitored internet environments in the world. In the context of the Arab Spring, many authoritarian governments either attempted to close down social media to inhibit uprisings or used surveillance and monitoring of such media – as also in Iran in 2009 – to track and suppress dissent.

In the United Kingdom, the draft Communications Data Bill has been rightly termed a 'snooper's charter'. If passed, the bill will demand the population-wide storage of information on British citizen's emails, text messages and internet activity. It would also represent the most intense surveillance and monitoring of a population by any democratic government to date and risks being used by authoritarian regimes as justification for their own surveillance practices. The British government is sending mixed messages by defending freedom of expression abroad, as Foreign Secretary William Hague did recently in his speech at the Budapest Conference on Cyberspace in October 2012. If it is to credibly defend online freedoms abroad, the UK must equally protect and promote those of its own citizens. While reasons such as tackling crime and terrorism have been used to justify the approach of the Communications Data Bill, there can be no justification for population-wide surveillance.

Western technology companies are also producing and exporting surveillance equipment that allows governments to retain data and spy on citizens. The mass surveillance industry is worth an estimated $5 billion per year, with much of this technology being exported to authoritarian states. The University of Toronto Munk School this year published research showing how Bahraini activists have been targeted using FinFisher, a piece of software sold by the UK-based company Gamma Group. One positive step was taken recently when the European Parliament endorsed stricter European export controls of such "digital arms", as proposed by Dutch MEP Marietje Schaake, though whether the EU's member states will follow this lead is open to question.

- **Mass monitoring and surveillance of citizens use of digital communications is a dangerous and unacceptable breach of fundamental human rights.**
- **Any government defending or standing up for freedom of expression in its own country and around the world must not undermine that free expression through mass surveillance.**
- **Urgent moves are needed to restrict the export of surveillance equipment and technology to states that do not respect human rights.**

Access to the Digital World

Access to freedom of expression in the digital world means more than just access to information. Access to the internet itself, quality of communication, affordability of service and the information and communications technologies needed to make practical use of the web all count. Media that serves all sectors of society, multi-cultural, multi-lingual, partisan and non-partisan, and in formats that help the disabled are also essential. "The power of the Web is in its universality," says Tim Berners-Lee, its inventor.

There remains a digital divide both within and between countries, notably in developing countries. Adequate infrastructure also remains an issue, especially in rural areas and regions of poverty, though the rise of mobile technology is starting to change the story. The Pew Internet Project[2] says: "Groups that have traditionally been on the other side of the digital divide in basic internet access are using wireless connections to go online." Many millions more will go online via mobiles in the next few years. It is vital that digital censorship does not close down these spaces just as more people access them. Nor must other obstacles to free expression online and off be allowed to persist, including illiteracy, marginalisation and poverty, or through discrimination by gender or by ethnicity.

Acting to ensure and encourage access to the digital world can help to support economic equality, social mobility, economic growth and democracy. It opens up a new and evolving public sphere where opinions can be formulated, shared and turned into consensus for mobilisation. It creates the possibility for a change in the way politicians and citizens exchange and debate ideas. Greater access shifts power from the leaders of nation states and their allies to individuals and networks of individuals, cutting across old hierarchies.

- **As the digital world becomes an increasingly important part of social, economic and political life, access to the internet and digital communications is fundamental.**
- **Ensuring free, uncensored access without discrimination or any form of political, social or economic blocks is vital.**

Human Rights Defenders and Citizen Journalism

The technological innovations that have transformed the work of activists and human rights defenders around the world work both ways. Ever more advanced tracking and surveillance online leads the police, paramilitaries (and other often unknown groups) to the doors of peaceful activists and ordinary citizens in repressive states. Attacks on bloggers, pervasive surveillance, hacking and manipulation of websites continue as authoritarian states push back against the growth of alternative networks outside their immediate control.

[2] See http://pewinternet.org/Reports/2012/Digital-differences/Overview.aspx

In 12 of the 47 countries reviewed by Freedom House[3] in 2012, new laws or regulations disproportionately increased the state's powers of surveillance or restricted user anonymity in the preceding year. In 19 of the 47 countries assessed, a blogger or internet user was tortured, disappeared, beaten, or brutally assaulted as a result of their online posts. Controls on political speech online – even expressed by Twitter or mobile phone text message – have led to arrests. In five countries, an activist or citizen journalist was killed in retribution for posting information that exposed human rights abuses.

In some democratic states as well as authoritarian ones, user rights and oversight rights are falling behind legal powers, leading to abuse. Paid commentators and state-endorsed hacking attacks are increasing. In Russia, massive distributed denial-of-service (DDoS) attacks and smear campaigns against activists have intensified. In Pakistan, there have been attempts to ban encryption and virtual private networks (VPNs) and mobile phone communications cut off for a day in Balochistan province. In Egypt and Azerbaijan, mobile phones and social media are still under vigorous surveillance and bandwidth speeds have been throttled to reduce access to social media, a space to share information and organise.

Yet as the censors advance, new opportunities, tools and techniques arise to protect and further the right of citizens and civil society create, disseminate and receive information, express opinions, to mobilise, coordinate and organise online. Tracking and reporting censored websites and monitoring the harassment of rights defenders communicating online has become vital work for free expression defenders.

Policymakers should act to support the sharing of technology that allows the user to circumvent surveillance and communicate and organise safely online and limit the export of monitoring technology to repressive states or governments that otherwise operate outside the rule of law to limit peaceful opposition. International communities of activists should be assisted as much as possible in their efforts to help human rights defenders develop, share and adopt security routines, online and in the real world, that are practical, effective and relevant to their local political environment.

Online media

Today more than ever, blogs and other social media publications allow the public to share and receive information, actively participate in government and get their voices heard. And as the mainstream media sheds reporting staff in a declining market, the historic role of the press in observing, reporting and calling authority to account increasingly falls to these citizen journalists.

But without the protection and legal resources of mainstream media institutions, citizen media can be easy targets for defamation actions and physical intimidation. This year Reporters without Borders recorded 123 cases where "netizens" were jailed for their online opinions in 12 countries. Nearly 70 are held in China alone. Nearly 40 Syrian citizen reporters have been killed covering the fighting in their country. Even in the US, historic First Amendment free speech

[3] See http://www.freedomhouse.org/report/freedom-net/freedom-net-2012

rights for bloggers are under threat by federal court rulings that say they are not entitled to the same legal protection that other members of the press enjoy.

- **As surveillance, filtering, cyber-attacks, website blocking and filtering, content manipulation and imprisonment of bloggers increase, human rights defenders need direct support in helping them better manage their physical and digital security risks in ways that are practical, effective and relevant to their local political environment.**
- **Online and citizen journalists must be given the same protection as mainstream and offline media organisations.**

Copyright

Copyright is one of the most contentious areas of internet governance. In September 2012, Google reported that it had received over 7,380,000 requests to remove copyrighted material from its indexes, with over 1,000,000 of those coming from the UK music industry alone. Music and film/TV sharing dominate the argument, but there are also countless livestreams of sporting events to be found online.

While it would seem clear that artists and performers deserve to be recompensed for their efforts, and broadcasters and publishers for their investments, measures such as ACTA (which was eventually thrown out by the European Parliament in July 2012) resemble sledgehammer legislation, designed to criminalise even fair usage of copyright material, and threaten both the culture and practices of the web.

The interconnected nature of the internet also make copyright arguments very complicated: does an aggregator site merely provide the same indexing service as a search engine, or does a site such as Megaupload actively publish, and encourage others to publish (and download) copyright material?

Different models such as crowdfunding have been tested by artists attempting to escape what many see as a business model that will not survive. As technological change continues apace and makes existing approaches to copyright appear increasingly infeasible, and as attempts to enforce traditional copyright in the digital world risk criminalising and censoring large numbers of individual users, there is a need for an open and thoughtful debate that looks at new business models that can work for artists/creators and users alike.

The issue of free downloading of copyright material has led some to suggest barring those who infringe copyright from the web, an issue that has serious implications for free speech and would constitute an undermining of fundamental rights.

- **Traditional copyright models and the technological opportunities of the online world are increasingly in conflict.**

- **Open debate is needed on new business models that can work for artists and for users in the digital world.**

Index's Key Recommendations

Internet Governance

- Establishing a global body exercising top-down control of the internet would risk increased censorship and suppression of free speech – not least given the number of countries and states already censoring and monitoring the net – and would be likely to severely erode openness and inhibit innovation and creativity.
- A multi-stakeholder, bottom-up structure of internet governance is a vital component of ensuring an open and free internet through which freedom of expression and other fundamental rights can be promoted and defended.

State and Corporate Censorship

- State and corporate censorship are increasingly threatening freedom of expression in the digital world. Neither states nor companies should be in the business of putting country or network-wide filters or firewalls in place with the aim of chilling or censoring free speech.
- Takedown requests should always be backed by a court order, and as with free speech offline any limits must be highly constrained and transparent.
- Intermediaries should not be made responsible for censoring content, and private companies should fully respect their human rights obligations in their operations around the world.
- Governments must not move in the direction of criminalising speech and digital communications in ways that will chill free expression and risk dampening the use and development of social media.

Surveillance, Privacy and Free Expression

- Mass monitoring and surveillance of citizens use of digital communications is a dangerous and unacceptable breach of fundamental human rights.
- Any government defending or standing up for freedom of expression in its own country and around the world must not undermine that free expression through mass surveillance.
- Urgent moves are needed to restrict the export of surveillance equipment and technology to states that do not respect human rights.

Access to the Digital World

- As the digital world becomes an increasingly important part of social, economic and political life, access to the internet and digital communications is fundamental.
- Ensuring free, uncensored access without discrimination or any form of political, social or economic blocks is vital.

Human Rights Defenders and Citizen Journalism

- As surveillance, filtering, cyber-attacks, website blocking and filtering, content manipulation and imprisonment of bloggers increase, human rights defenders need direct support in helping them better manage their physical and digital security risks in ways that are practical, effective and relevant to their local political environment.
- Online and citizen journalists must be given the same protection as mainstream and offline media organisations.

Copyright

- Traditional copyright models and the technological opportunities of the online world are increasingly in conflict.
- Open debate is needed on new business models that can work for artists and for users in the digital world.