Internet Society

CHATHAM HOUSE
The Royal Institute of International Affairs

A Brave New World: How the Internet Affects Societies

Professor Dr Erik Huizer

Chief Technology Officer, SURFnet; Research Associate, University of Utrecht; Internet Hall of Fame Inductee

Syed Ismail Shah

Chairman, Pakistan Telecommunications Authority

James Arroyo OBE

The Ditchley Foundation

Dr Unoma Ndii Okorafor

Founder & CEO, WAAW Foundation; Co-Founder & CEO, Radicube Technologies

Rebecca MacKinnon

Director, Ranking Digital Rights, New America

11 May 2017

The views expressed in this document are the sole responsibility of the speaker(s) and participants, and do not necessarily reflect the view of Chatham House, its staff, associates or Council. Chatham House is independent and owes no allegiance to any government or to any political body. It does not take institutional positions on policy issues. This document is issued on the understanding that if any extract is used, the author(s)/speaker(s) and Chatham House should be credited, preferably with the date of the publication or details of the event. Where this document refers to or reports statements made by speakers at an event, every effort has been made to provide a fair representation of their views and opinions. The published text of speeches and presentations may differ from delivery.

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

With the rise of the Internet in recent decades, its impact on society has been transformative at multiple levels – including in communication, access to knowledge and social interaction.

While early adopters saw possibilities in using the Internet as a vehicle through which the many challenges facing the world might be addressed, more recently questions have arisen about how Internet technology can be used to spread false and misleading information, and to radicalize and recruit potential terrorists. There are also concerns as to whether the Internet serves to reduce or exacerbate social divisions; and whether it contributes to the dilution of social norms or, conversely, serves as a channel to perpetuate them.

In this context, the technical community has initiated a conversation about the role that the Internet is – and should be – playing in societies. Notably, for some within the technical community, there is growing unease that the very technologies that supported Internet growth are also enabling behaviours that are socially unacceptable, putting pressure on the way people use and experience the online environment.

On 11 May 2017 the Internet Society and Chatham House convened a roundtable discussion, held under the Chatham House Rule,[1] at which a culturally and geographically diverse set of participants examined questions relating to how the Internet affects social norms and societies as a whole, as well as its impact on people's daily lives.

Access, capacity and the developing world

The Internet is for everyone, according to the Internet Society's vision, but it has not quite happened for all. Access to the Internet is essential for empowerment of certain groups, especially women, connecting them with global markets and communities. Yet, women in Africa are 50 per cent less likely to be online than men; and there are digital divides also affecting people with disabilities, and people lacking digital skills.

The Internet in the developing world

An Internet Society survey of 2,100 people across the world has found that people in developing markets remain optimistic that the benefits of connecting far outweigh the perceived risks. On the contrary, in the Western hemisphere, conversations about the Internet risk losing the sense of genuine excitement and urgency that many in developing countries feel about getting online.

The mobile Internet has been a game changer in developing countries. In Pakistan there were 3.79 million broadband connections through 3G in 2013. In just three years, however, the advent of 4G has increased the number of mobile broadband connections to 43 million. For regulators in developing countries, the first step is to bring people online, and after that to focus on new services. For example, graduates in Pakistan increasingly want to be entrepreneurs rather than be employed by others. Entrepreneurial activity, in turn, increases financial inclusion: Pakistan's vision is now that by 2020 50 per cent will have their own bank account.

[1] When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Digital divides

Connectivity is growing fast, but some places are not doing as well as others. ‘Access’ is not as simple as giving people connection to the Internet. There are multiple, multi-dimensional factors contributing to digital divides, chief among them gender, access to education and skills, lack of locally relevant content, lack of human capacity, and weak local supply chains. All these issues need to be addressed if the vision of the ‘Internet for everyone’ is to be achieved.

In particular, a lack of localized content risks turning Internet users from developing countries into consumers rather than creators. An estimated 90 per cent of jobs that will be created over the next decade will require technical skills, and Africa will be, in demographic terms, the youngest continent. There is an urgent need to develop relevant skills to both preserve and expand opportunities for all.

At the same time, technological innovations are further deepening divides. There is a risk that greater digital inequality will spread within countries – between those who are connected and those who are not. This inequality will affect jobs and the economic performance of countries and communities. In a scenario in which there is likely to be a threshold for innovation to see gains in the economy, without proper access and education many people will be left behind.

On the more positive side, the spread of Internet uptake can also work to address divides within societies. In Pakistan, for example, some 70 per cent of medical students are women, but for cultural reasons only 20–30 per cent of practising doctors are women – even though many female patients prefer to be seen by a female doctor. There are successful examples of using technology to bring women and girls into the workforce, for example by enabling women to access female doctors via remote consultations. As another example of the interplay between local and global, Pakistan is home to one of the world’s largest ‘virtual’ universities, established in 2002.

Trust and fear in the online environment: the ‘silent majority’ is vanishing

A case can be made that, in the ‘real’ world, the Chatham House Rule is comparable with the Internet Society’s vision of the ‘Internet for everyone’. The Rule is intended to ensure that people can speak openly and freely, but also securely. It provides a channel for an issue to be thoroughly debated, and this lends legitimacy. Members of the technical community may view confidentiality as secrecy, but on difficult issues people of good faith need some room to talk and interact freely.

Online debate

The confidentiality offered by the Chatham House Rule encourages people to speak freely, but its efficacy depends on physical meetings in the real world, at which the presence of a silent majority plays an important role in curbing extreme behaviour. No equivalent mechanism exists in the online environment: the silent majority is not only silent, but invisible. As a result, debate can spin out of control.

One speaker remarked that ‘fear is trumping trust’ online. It is important that people are able to speak freely online, but there is no shared moral and/or cultural code influencing how people behave. The risk, therefore, is that online debate is reduced to the lowest common denominator: ‘Civil debate according to the Chatham House Rule is hardly possible online. This leads to a sort of extreme behaviour in debates, which in turn leads to self-censorship.’

Real-world implications

A case can be made that in some instances hate speech may provoke actions in the real world that threaten the personal safety of many. In Rwanda, for example, where 'hate media' had a role in fuelling the genocide in 1994, the government is now attempting to restrict what is published online. In early 2017 the government of Cameroon blocked Internet access for the English-speaking part of the country for 93 days. The government said that it reserved the right to stop the Internet being used as a tool to stoke internal division and hatred. However, Internet filtering and shutdowns create extensive collateral damage, and have, in the case of Cameroon, for example, been condemned by the UN Special Rapporteur on freedom of expression as an 'appalling violation' of the right of freedom of expression.

Globalization and the Internet as an engine for economic growth

Governments around the world recognize that the Internet is an engine of growth. States are committed to connecting more people (1.5 billion by 2020, in line with the ITU target) to advance the gains that can be made from the Internet economy.

The evolution of the Internet, particularly from the 1990s, has coincided with the end of the post-war East–West order (the so-called 'end of history'), and the advance of globalization. Whereas diplomacy has traditionally depended on adapting behaviour to local culture in order to reduce friction, what is new is that the Internet effectively 'collapses' concepts of place, and, with that, the ability to hold separate value systems in different places.

The role of the state

Workshop participants discussed the appropriate role of the state in an increasingly globalized – but simultaneously fragmented – world. Explicitly Western values have driven the agenda to date, and states that do not buy into those values will view the Internet's advance as a direct threat. Internet policy dialogue tends to lump non-Western countries or governments together, as though they are all alike. However, there are certain 'rule-of-law' states that place more value on social responsibility and cohesion than on individual personal expression. The challenge for states is thus to figure out how to work together without necessarily quite agreeing on such values.

In the opinion of one speaker, quick change will be resisted and conflict is likely to occur. Another disagreed, contending that the Internet's values are aligned with the Universal Declaration of Human Rights.

There are conflicts between the principles of state sovereignty and globalization. Internet regulation is mostly confined within state borders, but both regulation and technical decisions can have global impacts. One participant asked if it remains accurate to view the Internet as a global network. Other participants noted that the Internet is not just creating challenges for regulation between states because of diminishing borders, but also within the national state bureaucracy. As regards the latter, the Internet has forced a change in the jurisdiction of certain agencies – for example, branches concerned with communication are now asking about their role in the privacy debate – and there is increasing strain placed on governments as these agency jurisdictions continue to blur.

The evolving security challenge

The growth of the Internet has been hugely disruptive to intelligence services. Disruption and encryption have bitten into traditional intelligence models. Agencies are now learning to embrace the Internet to deal with the evolving threats of terrorism and non-state actors. While acknowledging that bulk powers have their critics, one speaker expressed the view that the UK Investigatory Powers Act (2016) is modernizing how intelligence agencies collect evidence.

Threats

In the past, when government organizations thought about Internet security, they focused on the top 5 per cent of high-risk events, such as attacks on critical infrastructure. While potentially devastating, such attacks are rare compared with the constant barrage of cyber incidents affecting the population at large. As a result, governments are increasingly concerned with the Internet as it relates to civilian usage. Moreover, the evolution of the modern Internet has led to non-state actors, such as terrorists and hackers, posing security threats to states. Governments are still learning how to respect the privacy of individuals' communications in the context of criminal investigations.

One participant noted that there has been a 'market failure' in security, and that citizens are not managing risks sufficiently. The UK government, for example, has responded at the national level by creating the National Cyber Security Centre.

The Internet of things

The Internet of things (IoT) also poses a big challenge to security. In the next 10 years an estimated 30 billion connected devices will come online. The growth in IoT marketing and innovation has outpaced security, and there are no good economic incentives in place to promote security. Many traditional companies that had nothing to do with information technology are now in effect becoming IT companies, but do not understand how their products can create vulnerability in the network. In this context, how do we continue to connect more devices and gadgets to the network without creating further vulnerability and insecurity? The second challenge around IoT and security pertains to data collection. Most of the focus for regulation is on visible – or physical – things, such as actual devices and gadgets. One participant suggested that as IoT exists in the cloud, that is where security and privacy solutions may be effective.

State regulation in a global world

One speaker described the present situation as a 'Magna Carta moment' – a general realization that 'we don't have the right structures to address the problems we're facing'. 'The nation state system of governance … for national and international and corporate governance are not fit for purpose to deal with the issues we're facing.' There is a need to bring together the right stakeholders to address the problems.

Regulation

Other participants noted that regulation by the state can resolve many of the current problems, such as market failure around security.

When governments make local laws, they need to recognize that they are part of a broader, global system. Therefore, in one speaker's view, governments need to be accountable not only to their own people, but to everyone on the network.

Others advocated less regulation, making the case instead for raising awareness of the opportunities the Internet brings. One participant asked if governments should be more visible in Internet regulation. Should there be a 'complaints department' for consumers at a national level, for example? Or should companies be forced to be more open by allowing algorithms to be reviewed by regulators to help prevent bias? Another noted that the media and the public sphere have become less transparent, and if the state does not play a part in regulating private companies, the data they collect, and the algorithms they operate, then there will be an imbalance.

Democracy and corporate power

Events in 2016 brought surprises in terms of democratic outcomes. Notably, following the Brexit referendum in the UK and the outcome of the US elections, many people are worried about the role of social media in creating filter bubbles and echo chambers, and in spreading fake news.

Extreme behaviour

One speaker raised the point that the vast majority of extreme behaviour is played out on two platforms with the largest user bases. There have been numerous attempts to develop norms of behaviour, or create technical solutions that could filter extreme material. It was only when advertisers started to abandon the platforms because they saw their brands being damaged by association that the platforms did anything about it.

The role of companies

While there has been increased transparency about how companies are responding to requests from governments for user data, there is little publicly available information about firms' internal processes to moderate content on their platforms. Companies have done a good job in removing images of child abuse, for example, but a poor job in relation to images of breast feeding, or nudity in art. There is also a concern that, where governments are putting pressure on social media companies to take down allegedly extremist material, this may unjustifiably also target the work of human rights activists and journalists.

As recently as 2011, the discussion about the relationship between social media and democracy would have been very different. One participant noted that social networks were initially viewed as a democratizing force, but now the world is seeing the negative impacts that social media can have on society. One participant framed this as a transition from an 'algorithm-less' world to one that is 'algorithm-full'. Another participant noted that, previously, the algorithms used to provide consumers of social media with information were often viewed as neutral. However, events in 2016 have changed people's perspectives on how social media algorithms can create bias and perpetuate false information. Although the Internet feels like a public space, it is built on private infrastructure; and the companies that control these algorithms hold a great deal of unaccountable power.

Encoding values into the online environment

Just as the Internet Engineering Task Force (IETF) had to adapt to the internationalization of its membership by adopting a code of conduct, there is an urgent need to find an equivalent set of norms to enable 'civilized' debate online and reduce extreme behaviour.

While technical solutions seem attractive, it is important to be aware of both the opportunities and risks of encoding social values into algorithms, or into machines themselves. This process will reach its zenith with autonomy, but machine learning biases are already apparent. How can there be a distributed system that is secure, when security itself is a value judgment?

Legitimacy in the multi-stakeholder process

Internet governance began as a technical project but ended up in the world of policy. The technical community has often been very open and transparent, whereas government decisions are often made under conditions of confidentiality. In this context, questions were asked as to how we get these two very different communities to work together and within the confines of traditional institutions; and who should be responsible for convening this consultative space.

A new status quo

Intelligence services used to assume that the status quo would remain of the Internet as a global commons. This view was challenged in 2010, in light of a raft of proposals for new international laws, protocols and technologies designed to benefit authoritarian states. Since then, engagement through the Internet Governance Forum has been stronger; but a liberal, multi-stakeholder perspective is not guaranteed, and will need to be fought for.

Multi-stakeholder policies

Internet policy has become divorced from public-sector spending rounds in many countries, for example in the UK. In this context, multi-stakeholder policy can be undertaken, but only if it does not have a financial impact. One participant noted that discussions on Internet governance and enhanced cooperation tend to go round in circles. In other countries, such as in Malaysia or Kenya, progress on multi-stakeholder models has been reversed when governments have changed or instability has increased. It is unclear who the convenor of the open, consultative space is.

One speaker asserted that while the multi-stakeholder model is liberal, it is not democratic, and there is a danger that in certain environments only the 'right sort' of stakeholders are wanted. One participant argued that there is little legitimate input by civil society, whose voice has been crowded out. Another disagreed, noting that those who exert most influence are people who have gone beyond the normal range of effort to extend their expertise.

There is therefore a complex 'ecosystem', and different types of decision-making are needed for different problems online. One participant noted that the Internet community has reinforced how the multi-stakeholder model can work. But the role of the public and of civil society is important in demanding systematic change in how governments make decisions that affect the Internet.

What are the solutions to current and foreseeable challenges?

As one speaker remarked, there is not a ‘grand, top-down plan that we will suddenly innovate. It will evolve organically in a very “Internet-y” way.’

Possible solutions

International norms for behaviour and security
Several speakers highlighted the need for norms of online behaviour and security. This challenge should not be underestimated. The collapse of place is something new, and this challenges the ability to hold separate value systems in different places – something that has previously been essential for successful international diplomacy.

Technical solutions to make visible the silent majority
Technology cannot solve problems of human behaviour, but the problems cannot be solved without technology. The knee-jerk reaction has been to call for unwanted material to be blocked, but the minute this starts, filter bubbles are created. An alternative approach may be to adopt public broadcast values – whereby all views are presented and consumers are necessarily confronted with a range of viewpoints. One speaker suggested that technology could be harnessed to track who reads discussions.

Accountability for corporate impact on human rights
One solution may be to develop benchmarks for companies to make commitments; for others to be able to assess whether those are the right sort of commitments; and to provide data that will enable policymakers, civil society, companies and investors to have a conversation about what sort of Internet is collectively wanted.

Hate speech and fake news
Several speakers agreed that organizations like the Internet Society could help by starting to have essential conversations around fake news, hate speech and extremist content.

Security and the Internet of things
Regulators need to consider who holds IoT data, and focus on the cloud rather than attempting to regulate every object that comes onto the market.

Progress is possible, but the risks are real
One speaker noted that many of the problems that are hotly debated in the context of Internet policy have affected humanity for generations. These problems arise from success not failure. Traditional institutions such as the judiciary have shown themselves to be able to deal with many issues. Previous leaps forward in human connectivity have also led to unprecedented human destruction. Nevertheless, progress has been made, and ‘humanity has evolved’. In the long run, things are improving, and there are great possibilities for innovation, development and human growth.

The developing world is hopeful

Speakers from the developing world emphasized that for many developing countries the Internet continues to be seen overwhelmingly as a medium of opportunity and empowerment. Although countries in the developing world understand that the Internet can impose challenges on society, they still feel that the Internet is the only existing medium that can efficiently provide effective solutions to issues such as poverty, marginalization and education. Some participants also noted that the acceleration of technology could lead to a deepening of existing inequalities, but asserted that this risk could be overcome through truly inclusive and participatory processes.