The internet, governance and fundamental rights

Alan Finlay and Joy Liddicoat

We at the Association for Progressive Communications (APC), along with other civil society commentators, have been calling for the reinvigoration of the 'internet access debate', placing primacy once again on those who are excluded from participation, and on the implications of internet access for securing rights, such as the rights to education and health and to the benefit of science. There is a need for this debate, particularly in developing countries, and a need to renew thinking on the potential impact the internet can have on our lives and society. APC has also been engaged in advocacy that pushes for internet access to be recognised as a human right, as part of the global human rights framework.

It is with regard to this second concern, the internet and human rights, that the idea of what the internet is and what it means to us has shifted. By advocating for the internet to be integrated within the human rights framework, we are implicitly pointing to its ubiquity and pervasiveness in our everyday lives, and the need to understand it in this context.

Surveillance and proportionality

An internet rights discourse has been provoked by recent evidence of state and private sector surveillance of the internet.[1] In South Africa, the monitoring of two investigative journalists by state officials has shown how civil liberties are easily undermined, despite constitutional guarantees to the contrary (Duncan, 2014). As Duncan writes: 'South Africa is not a terrorist target, yet growing social protests mean that the temptation is there for less principled members of the security apparatus to abuse the state's surveillance capabilities' (*ibid*). Zimbabwe, like many countries that covertly or brazenly push through surveillance laws, similarly shows how these laws can stand in contradiction to basic rights, often creating legislative incoherence: 'And as things stand there is discord in the legislative framework caused by disharmony between the statutes and the constitution, providing fertile ground for violation of citizens' basic liberties including their right to privacy' (Ngwenya, 2014).

In Bangladesh, Sarker and Hasan argue that an alternative to an 'authoritarian' model of surveillance is one that seeks to 'make people aware of the risks, to develop their capacities and to set down punitive measures that require proper evidence and respect individual rights'. However, 'Bangladesh is often swinging between these two models, and there is a sense in which it is addressing the situation on an ad hoc basis' (Sarker and Hasan, 2014). And, to take a non-Commonwealth South Asian neighbour as an example, in Nepal, internet service providers are pushed into filtering content, and monitoring high-bandwidth internet users (Pradhan, 2014).

Two things are apparent from these reports. Firstly, as with the orientation of the internet within a human rights framework, the emphasis by states on surveillance is symptomatic of how ubiquitous the internet has become in our lives. Secondly – and it feels unlikely that this could have been anticipated or desired by those doing the surveillance – this surveillance has reinvigorated fundamental ethical debates about how we interact as a society.

What kind of society do we want?

These debates are fundamental in that they have been around far longer than the internet, and are about the necessary boundaries of human interaction that make society possible – or the kind of society we may want. They are less about the internet, and more about *us*. What seems noticeable in some of these discussions is that there appears to be a careful re-thinking of why some rights matter in the first place. A good example of this is Glenn Greenwald's recent talk 'Why Privacy Matters', in which he said:

> *There's a reason why privacy is so craved universally and instinctively. It isn't just a reflexive movement like breathing air or drinking water. The reason is that when we're in a state where we can be monitored, where we can be watched, our behaviour changes dramatically. The range of behavioural options that we consider when we think we're being watched severely reduce. This is just a fact of human nature that has been recognised in social science, literature, religion and virtually every other field of discipline.*
>
> *There are dozens of psychological studies that prove that when somebody knows that they might be watched the behaviour they engage in is vastly more conformist and compliant. Human shame is a very powerful motivator, as is the desire to avoid it. For this reason when people believe they're being watched, they make decisions based on the expectations that others have of them or the mandates of societal orthodoxy rather than as a by-product of their own agency.*

States have been slow to engage with internet-related human rights discussion. Public policy-making in this area is fraught with difficulty. Legislators and policy-makers must work at the interface of telecommunications infrastructure regulation, national legal frameworks and the fast-paced nature of technological development, alongside rapid innovation on how citizens are using technology in their everyday lives. When combined with the legacies of colonial legislative frameworks, the challenges of parliamentary law-making processes and a lack of best practice guidance, the task of policy-makers is complex and challenging.

In Jamaica, where there is a high rate of violent crime, powers to intercept and to request telecommunications information, including internet-related communications data, may be critical to criminal investigations and prosecutions. However, as Dunn and Brown show in their article on a high profile court case in Jamaica, legislation imposing obligations on telecommunications companies

to share users' private information with law enforcement must be interpreted narrowly in order to uphold rights to privacy (Dunn and Brown, 2014, pp. 138–141). More work is needed to support discussions at national levels about the powers that should be granted to law enforcement agencies in ways that uphold and secure citizens fundamental human rights, including the right to privacy (*ibid*, p. 141).

Yet there are very few resources for policy-makers in this area. For example, there is little best practice guidance on internet-related regulation, and still less on how to take account of human rights in relation to the internet. Commonwealth countries that participate in the global Internet Governance Forum[2] or that participate in national internet governance forums have much better access to best practice and can share issues and test ideas alongside other stakeholders including civil society, the technical community, academics and the private sector.

Too often in the last five years, approaches to internet-related policy-making have been exclusively from the entry points of cybercrime and national security, with the result that multi-lateral agreements on information sharing, counter terrorism measures and even trade-related issues have been at the forefront of shaping responses to law and technology. Human rights, including the rights to freedom of expression and privacy, have not been adequately considered. It is incredible, for example, that it was not until 2012 that the United Nations Human Rights Council passed its first-ever internet-related human rights resolution. The resolution, supported by 80 states, affirmed the simple concept that 'the same human rights people have offline must also be protected online' (UNGA, 2012).

Right to privacy

In June 2014, however, the out-going High Commissioner for Human Rights, Navi Pillay, released a ground-breaking report on the right to privacy in the digital age (OHCHR, 2014). Prompted by concerns about mass surveillance by some states, and responding to a call from the United Nations General Assembly to investigate the matter, the commissioner's report hails a new era in human rights and the internet which will be of critical importance to policy-makers.

With careful analysis based on more than 50 submissions, the report makes five main findings and recommendations:

- Mass surveillance by its very nature interferes with the right to privacy, regardless of whether such data is used, and also interferes with other human rights. Surveillance measures must be necessary and proportionate
- Imposition of mandatory retention of third-party data on private companies is neither necessary nor proportionate and therefore violates human rights
- Inter-governmental intelligence-sharing regimes are contrary to human rights law: 'secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of law'
- Human rights apply regardless of frontiers and without discrimination – governments cannot avoid human rights obligations on grounds of extraterritoriality
- Business and the private sector have been facilitating surveillance and must take more action to uphold human rights (specifically drawing on the Guiding Principles on Business and Human Rights)

The implications of this report and related developments are profound and Commonwealth countries need to engage and support each other in responding to these new and emerging human rights issues. The Charter of the Commonwealth reaffirms the importance of democracy, human rights, the separation of powers, the rule of law and good governance, and the role of civil society. A more detailed discussion is needed about the state of internet-related human rights and the prospects and challenges for rights affirming responses. At the same time, technical assistance and support is needed in order to continue building high quality, affordable internet access for all.

Endnotes

1 Examples include revelations by Edward Snowden, see also reports by Global Information Society Watch 2014 (available at: www.giswatch.org), among others.

2 The Internet Governance Forum is United Nations mandated, see: http://www.intgovforum.org/cms/

References

Duncan, J., 2014. 'Communications surveillance in South Africa: The case of the *Sunday Times* newspaper'. *Global Information Society Watch 2014: Communications surveillance in the digital age*. Montevideo: APC, Hivos. pp. 224–227.

Dunn, H. and Brown, A., 2014, 'Resisting citizen data handover in Jamaica: The case of Digicel vs INDECOM'. *Global Information Society Watch 2014: Communications surveillance in the digital age*. Montevideo: APC, Hivos. pp. 143–146.

Greenwald, G., 2014. Why Privacy Matters [webpage] TED. Available at: www.ted.com/talks/glenn_greenwald_why_privacy_matters/transcript?language=en [Accessed 9 December 2014].

ALAN FINLAY is the editor of *Global Information Society Watch* (www.giswatch.org), an annual report published by the Association for Progressive Communications (APC) and Hivos. He is a freelance researcher, writer and editor, and has spent the past 14 years working in the non-profit sector on issues including media rights, environmental sustainability and progressive internet policy. He lectures in development communication at the University of Witwatersrand in Johannesburg.

JOY LIDDICOAT is a human rights lawyer specialising in ICTs for the Association for Progressive Communications (APC). A former commissioner with the New Zealand Human Rights Commission, she has worked in diverse public, private and civil society organisations at national, regional and global levels. Liddicoat participates in the Non Commercial Users Constituency of Internet Corporation for Assigned Names and Numbers (ICANN) and was a councillor on ICANN's Generic Names Supporting Organisation Council from 2012–2013. She completed her LLM (Distinction) at Victoria University, Wellington in 2010 on domain name dispute resolution. She currently serves as vice president of InternetNZ.

Ngwenya, N., 2014. 'Surveillance under the garb of rule of law'. *Global Information Society Watch 2014: Communications surveillance in the digital age*. Montevideo: APC, Hivos. pp. 280–283.

OHCHR (Office of the High Commissioner for Human Rights), 2014. *The Right to Privacy in the Digital Age* [webpage] OHCHR. Available at: www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx [Accessed 5 December 2014].

Pradhan, K., 2014. 'Somebody's watching me?' *Global Information Society Watch 2014: Communications surveillance in the digital age*. Montevideo: APC, Hivos. pp. 174–177.

Sarker, P. and Hasan, M., 2014. 'Online spaces, privacy and surveillance in Bangladesh'. *Global Information Society Watch 2014: Communications surveillance in the digital age*. Montevideo: APC, Hivos. pp. 72–75.

UNGA (United Nations General Assembly), 2012. *The promotion, protection and enjoyment of human rights on the internet* [webpage] United Nations. Available at: http://daccess-ods.un.org/TMP/8080236.91177368.html [Accessed 5 December 2014].