6

Human rights and the new(ish) digital paradigm

Gaia Marcus

To call the internet and its accompanied increase in computing capabilities a 'new' phenomenon would be something of a misnomer – the internet has been in development since the 1960s, and became publically available in August 1991. However, the globalisation of communications, associated erosion in state borders and dizzying acceleration of technological advancement over the past two decades have fundamentally changed the citizen-state relationship, introducing new actors, new platforms, new opportunities and new threats.

Whilst it is beyond the scope of the chapter to define this new(ish) digital paradigm, several characteristics are highlighted. First, the weakening of the nation state both as a concept and as a geographical entity with borders that can be protected physically. Second, the ascendance of new global actors that dwarf nation states in budget, reach and technological know-how. Third, the creation of a globalised communications infrastructure (the internet!) that is multi-channel and subject to rapid flux. Fourth, the exponential increase in computing capabilities, which opens up new possibilities for data capture and analysis- from big data to social network analysis. As noted by Kaku 'Today, your cell phone has more computer power than all of NASA back in 1969, when it placed two astronauts on the moon' (2011, 21). This (thoroughly incomplete) chapter is intended to stimulate further thought and debate with regards to applying this new(ish) digital paradigm to our understanding of human rights and the ways in which human rights defenders implement programmes and hold states and other actors to account.

Digital human rights?

The concept of digital rights tends to encompass how the new(ish) digital paradigm adds new dimensions to existing rights, and this will be the focus of the following section. A separate area of enquiry (not touched upon here) is examining whether new rights are created by the new(ish) digitised paradigm in which we live. For example, what would a 'right to the Internet' look like?

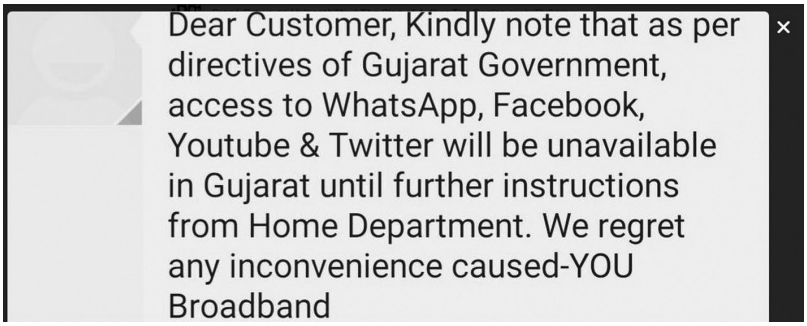

Figure 1. Example of state mandated blocking of the internet in Gujarat; screenshot of picture shared on Twitter taken by author, all identifying information has been removed. See BBC (2015).

There is precedent: internet access is now protected in certain legal systems (Lucchi 2011). Similarly, individuals' right to access information 'regardless of frontiers' is currently a subset of Article 19 of the Universal Declaration of Human Rights (UDHR). What might a 'right to access information' look like as a right in and of itself given the 'massive blocking, throttling, and filtering of the internet'[1] and the impact this has upon citizens?

Digital rights: some usual suspects

For Souter (2012), the articles most commonly understood by human rights professionals as being affected by the internet are articles 18, 19 and 20 of the UDHR – the rights to freedom of conscience, expression and association, respectively.

In the positive, it is now easier to share and access information, with more and easier channels for disseminating facts and views. The right to association can now also be a virtual right, with exchange happening across borders, using mediums ranging from text messaging to teleconferences. The current Syrian and Mediterranean refugee crises have seen both refugees using Facebook forums to understand where it is safe to cross borders and where to go, and European citizens using Facebook, Twitter and other online forums to self-organise and respond.

In the negative, an increased reliance on digital channels risks exacerbating the marginalisation of those without the digital or technical literacy to participate, or even the linguistics or literacy skills to navigate a mainly text-

1 United Nations Office of the High Commissioner for Human Rights, *Human rights, encryption and anonymity in a digital age* (1 July 2015). Available at http://www.ohchr.org/EN/NewsEvents/Pages/HRencryptionanonymityinadigitalage.aspx#sthash.FmDjxYec.dpuf (accessed 9 Oct. 2015).

based interface. For example, moves to shift online all job listings or voting systems, or access to state services such as health or pensions, greatly affect those who cannot (or do not wish to) use such platforms.

Online threats, offline impacts

New technologies are leading to new and increasingly more covert ways in which these rights can be curtailed. These include the blocking and intercepting of communications and channels (Figure 1), and can entail wholesale interception of all communications. While this is in theory possible with any remote method of communication – from intercepting post to scrambling radio signals – digital methods mean that far more can be done with far less man-power.

Online threats to rights such as the freedom of expression can have far more serious offline repercussions to human rights defenders and citizens given the enhanced potential for surveillance and locating actors using digital methods. These, sometimes deadly, threats can come from both state and non-state perpetrators. A recent case involved Mexican militia locating human rights defenders who were active online using both social media and offline pressure. The murder of the Mexican *Valor por Tamaulipas* journalist featured a particularly gruesome twist: her own social media accounts were used to announce and broadcast her murder (BBC 2014). Where states are involved, online surveillance can lead to mass state suppression, such as following the 'Arab Spring' in Egypt (McPherson and Alexander 2014). The very threat to life and basic freedoms places new responsibilities on human rights defenders and other actors, as the UN Special Rapporteur on freedom of opinion and expression, David Kaye, highlights:

> We live in a world in which mass and targeted surveillance, digital attacks on individuals and civil society, harassment of members of vulnerable groups, and a wide variety of digital opinion and expression result in serious repercussions, including detention, physical attacks, and even killings.[2]

Digital rights: some more unusual suspects

New channels lead to new ways in which rights can be violated, some of which may not be obvious at first. For example, the rights to non-discrimination and to a free and fair participation in society are at risk. Further, data protection and the right to privacy and private life are ever more at risk from excessive state surveillance and a largely unchecked global data-farming industry that is far more advanced in its science than most national governments (Venkataramanan 2015).

2 Ibid.

A tyranny of algorithms?

An overlooked, but potentially fertile line of inquiry would be the way in which the internet affects the right to non-discrimination: enter the algorithm.

Almost everything that you see on a responsive website – a website where content is not static, but tailored to the user – is a result of an increasingly complex set of algorithms. They tend to be geared towards efficiency, which often means revenue. This is why sites such as Amazon recommend new purchases or books to you, and explains why you are followed around the internet by adverts displaying products you have recently viewed. It affects your search results, the news you see, your experience of social media and much more.

A recent Google scandal highlighted what this means in practice. Datta, Tschantz and Datta (2014) found that men were shown adverts that advertised roles with large salaries more frequently than women. It is unclear from the research 'where' the gender based discrimination 'occurred', whether within the advertiser's brief to Google or within the way in which internet users were selected by Google to view the adverts. What the case did highlight, however, is the way in which algorithms can tend towards re-trenching existing inequalities and associated discrimination. In this case there was a retrenchment of societal trends that lead to men being more highly paid than women, but the basic mechanics are applicable to any bias that has its basis in social structures.

Recent cases have highlighted how online targeting and interactions – driven again by algorithms – can have offline repercussions. Facebook, for example, is able to increase voting in a geographical area through increasing the visibility of others having voted. Whilst an experiment that increases voting may seem like no bad thing, imagine the consequence to our right to free and fair elections if this targeting only happened in areas where a certain political party was particularly strong. There should be more attention paid to what we see on the internet, and the decision making processes or algorithms behind it. Nothing we see online is 'neutral' and more scrutiny needs to be placed on the human rights implications of that.

Too boring to fight for?

The technicality of the debate can be a key barrier to human rights activists and scholars truly engaging with the new(ish) digital paradigm. Concepts such as 'net neutrality' – the idea that it should not be possible to make it easier or cheaper to access certain parts of the internet – have key repercussions on our ability to use the internet for free expression and association. For example, the European Commission (2015) currently highlights the way in which service providers slow down (or 'throttle') service on free Voice over Internet services, e.g. Skype, pushing traffic to paid for services. The way in which service providers or states (e.g. see Figure 1) are able to control platforms that are

used by citizens for association and communication is clearly worthy of further analysis.

The right to privacy, contained within Article 12 of the UDHR, is another field of study that is currently limited to more technologically literate commentators and campaigners (Bélanger and Crossler 2011), or those specialising in information law and related disciplines. However, this could be an interesting area for further research, especially by researchers approaching it from a more conceptual angle. Indeed, the right to privacy is now a key area where balancing competing rights and principles such as proportionality come to the fore.

Civil society groups such as the UK 'Open Rights Group' or 'European Digital Rights' will focus on the ways in which online surveillance curtails rights. However, some element of state surveillance of communications could now be seen as being a fundamental component of states preserving fundamental rights and public order. What might the correct approach be towards derogating from certain rights? How have these played out in different regimes? Further analysis could shed interesting light: why do some states take a permissive line such as Germany's, and others a state surveillance heavy line such as the UK? Indeed, while the German Federal Constitutional Court ruled against the legality of 'the state [collecting] computerised data about a section of the population […] in order to identify potential subjects for surveillance' in 2006 (Youngs 2008, 331), the UK's position has led the UN Human Rights Committee to recently recommend that the UK 'should review its counter-terrorism legislation in order to bring it into line with its obligations under the Covenant.'[3]

Acting and holding actors to account

The new(ish) digital paradigm affords human rights defenders and scholars with new ways to hold duty bearers to account and fight for the completion of rights. These can range from the methods used to evaluate whether rights are being infringed, and how, to new awareness-raising mechanisms; for example, using websites such as http://www.eyesondarfur.org, or the current trend for petitions and associated 'clicktivism', or using very widespread web tools such as Facebook to respond to humanitarian crises.

Using quantitative data analysis to hold states to account

The statistical analysis of large datasets can offer insight as to the fulfilment of rights at a local, regional, national and international level. For example, the

3 United Nations Human Rights Committee (2015). *Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland* (advance unedited version) (Geneva: United Nations), available at http://www.equalityhumanrights.com/sites/default/files/uploads/Pdfs/CCPR_C_GBR_CO_7.pdf (accessed 9 Oct. 2015).

Centrepoint Youth Homelessness Databank project is creating an open data source for the UK about youth homelessness. The aspiration is to collect all available data on youth homelessness, open the data up using an interactive website, and perform analyses using it. This will allow insight into how rights to housing are being fulfilled, and if there are any specific demographic groups who are most affected by homelessness.

Compiling and aggregating data is a useful way of contrasting official statistics and rhetoric, and trying to delve into the problem at hand. A little data can go a long way. With incomplete data, collected through a Freedom of Information request, the Databank showed that eight times more young people ask the state for help in England and Wales than those who are officially being supported with housing by the state – this is equivalent to 136,000 young people seeking support and only 16,000 accessing their full legal entitlement to housing. This suggests that a significant majority of young people at risk of or experiencing homelessness in England and Wales are not adequately accessing their 'right to a standard of living adequate for [their] health and well-being', as per Article 25 of the UDHR (Centrepoint 2015).

Using network analysis to understand power structures?

Network analysis is a way of identifying actors and analysing the ties between them: kinship, friendship, reporting relationships, money flows and so on. Skye Bender-deMoll (2008) provides an excellent overview of the types of relationship that can be studied and some network basics. The RSA (Royal Society for the Encouragement of Arts, Manufactures and Commerce) has carried out extensive work on using network analysis to understand marginalised communities, identifying key actors and then working with them to plan local interventions (Rowson et al. 2010; Marcus 2011; Parsfield et al., 2015).

As a tool, network analysis allows the researcher to shed light on some of the key tenets of the human rights based approach: understanding underlying power structures; highlighting who the most disenfranchised are; and schematising how the intervention will affect social and other structures. Further, when analysing human rights violations, it is critical to understand the relationship between various actors and the networks of command or control that underpinned them.

Whilst network analysis is a burgeoning field in its own right, it can often feel daunting and time consuming to the newcomer. New tools that use tablet computers to store, code and analyse the data, even without internet access are becoming more viable. Any human rights scholar interested in pursuing this further should look into two open-source projects currently looking for collaborators: Rand Corporations 'EgoWeb' project or the University of Kentucky's 'OpenEddi' project.

Crowd-sourcing data and social media research

The ability to crowd-source a large amount of data, rapidly, can lead to better project planning, implementation, evaluation and monitoring. Live data can be used to understand where problems are worse, to track ongoing progress and to evaluate change over time. Sourcing data from social media can be used to hold duty bearers to account, for example, mapping human rights violations or humanitarian crises.

The Ushaidi project, for example, was initially deployed in Kenya in 2008 to map reports of post-election violence that were compiled from individual text messages and verified. The Peta Jakarta project, whilst using a similar method of collecting, verifying and mapping citizen reports (this time through Twitter), is used by Jakartan authorities and citizens alike to map flooding and make decisions on resource allocation and disaster responses based on real-time data.

Whilst the potential for using big data sources such as social media is clear, the ethics of using social media data are far murkier (McPherson and Alexander 2014). What does informed consent look like? How far can we trust the data – verifying reports is complicated, costly and sometimes inconclusive? Is it justifiable to collate and keep data without specific consent from the data subjects?

More starkly, what do we do with the data we are collecting: might we be putting people at risk through poor encryption or anonymisation (see McPherson 2014, and the Human Rights in the Digital Age project)?[4] This problem is at all levels: as highlighted by the UN Special Rapporteur on freedom of opinion and expression, there is currently no safe way of individuals contacting the UN to report violations.[5] Human rights institutions do need to play technological catch-up to retain their relevance.

Human first, digital second

This chapter has provided an incomplete overview of questions and challenges when applying our new(ish) digital paradigm to the international human rights regime. It has been squarely based on my own expertise and context, without seeking to look at the bleeding edge or darker corners of technology: blockchain technology, artificial intelligence, semantic or natural language processing, drones, the dark web, and others.

4 Centre for Governance and Human Rights, *Human Rights in the Digital Age*, available at http://www.cghr.polis.cam.ac.uk/research-themes/human-rights-in-the-digital-age-1 (accessed 8 Oct. 2015).

5 United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, UN Doc. A/HRC/29/32 (22 May 2015).

I have suggested some avenues for investigating digital rights, and new methods that can be used to both analyse the fulfilment of human rights and to hold rights bearers to account. This is a field in constant flux, and a field that sorely needs more scrutiny from those interested in the human first, digital second. Please do join us!

Bibliography

BBC (2014) *#BBCtrending: Murdered for tweeting in Mexico?* (27 October 2014), available at http://www.bbc.co.uk/news/magazine-29746651 (accessed 8 Oct. 2015).

BBC (2015) *Why has India blocked mobile internet messaging?* (27 August 2015), available at http://www.bbc.co.uk/news/blogs-trending-34074466 (accessed 8 Oct. 2015).

Belanger, F. and R. E. Crossler (2011) 'Privacy in the digital age: a review of information privacy research in information systems', *MIS Quarterly* 35 (4), pp. 1017–41.

Bender-deMoll, S. (2008) *Potential Human Rights Uses of Network Analysis and Mapping – A report to the Science and Human Rights Program of the American Association for the Advancement of Science*, available at http://skyeome.net/wordpress/wp-content/uploads/2008/05/Net_Mapping_Report.pdf (accessed 8 Oct. 2015).

Centre for Governance and Human Rights, *Human Rights in the Digital Age*, available at http://www.cghr.polis.cam.ac.uk/research-themes/human-rights-in-the-digital-age-1 (accessed 8 Oct. 2015).

Centrepoint (2015), *The Youth Homelessness Databank: Beyond Statutory Homelessness* (London: Centrepoint), available at http://www.centrepoint.org.uk/media/1690269/0054_yhd_report_full_v12.pdf (accessed 4 Dec. 2015).

Datta, A., M. C. Tschantz and A. Datta (2014) *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination,* available at http://www.degruyter.com/view/j/popets.2015.1.issue-1/popets-2015–0007/popets-2015–0007.xml (accessed 8 Oct. 2015).

European Commission (2015) *Net Neutrality Challenges*, available at https://ec.europa.eu/digital-agenda/en/net-neutrality-challenges#Article (accessed 8 Oct. 2015).

Kaku, M. (2011) *Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100* (New York: Doubleday).

Lucchi, N. (2011) 'Access to network services and protection of constitutional rights: recognizing the essential role of internet access for the freedom of expression', *Cardozo Journal of International and Comparative Law* 19 (3), pp. 645–78.

Marcus, G., T. Newmark and S. Broome (2011) *Power Lines* (London: RSA).

McPherson, E. (2014) *Human Rights in the Digital Age* (video) (Cambridge: Centre of Governance and Human Rights, University of Cambridge), available at http://www.cghr.polis.cam.ac.uk/research-themes/human-rights-in-the-digital-age-1 (accessed 15 Oct. 2015).

McPherson, E. and A. Alexander (2014) *Written Evidence for the Social Media Data and Real Time Analytics Inquiry* (London: Science and Technology Committee (Commons)), available at https://www.academia.edu/7621298/Written_evidence_submitted_to_the_Science_and_Technology_Committee_Commons_for_the_inquiry_on_social_media_data_and_real_time_analytics (accessed 15 Oct. 2015).

Parsfield, M.ed with D. Morris, M. Bola, M. Knapp, A.L. Park, M. Yoshioka and G. Marcus (2015) *Community capital: the value of connected communities* (London: RSA).

Rowson, J., S. Broome and A. Jones (2010) *Connected Communities: How social networks power and sustain the Big Society* (London: RSA).

Souter, D. (2012) *Human Rights and the Internet: A review of perceptions of human rights organisations. Report to the Association for Progressive Communications*, available at https://www.apc.org/en/system/files/HumanRightsAndTheInternet_20120627.pdf (accessed 15 Oct. 2015).

United Nations Human Rights Committee (2015) *Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland* (Geneva: United Nations), available at http://www.equalityhumanrights.com/sites/default/files/uploads/documents/humanrights/UN/CCPRC%20GB%20concluding%20observations%20(1).pdf (accessed 15 Oct. 2015).

United Nations Human Rights Council (2015) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, UN Doc. A/HRC/29/32 (22 May 2015).

United Nations Office of the High Commissioner for Human Rights (2015) *Human rights, encryption and anonymity in a digital age* (1 July 2015), available at http://www.ohchr.org/EN/NewsEvents/Pages/HRencryptionanonymityinadigitalage.aspx#sthash.FmDjxYec.dpuf (accessed 9 Oct. 2015).

Venkataramanan, M. (2015) 'Revealed: How free apps eavesdrop on your entire private life', *Wired* (14 July 2015), available at http://www.wired.co.uk/magazine/archive/2015/08/start/infoporn-free-apps-are-giving-away-your-private-life (accessed 8 Oct. 2015).

Youngs, R. (2008) 'Germany: shooting down aircraft and analyzing computer data', *International Journal of Constitutional Law* 6 (2), pp. 331–48.

Websites and avenues

https://www.openrightsgroup.org

https://edri.org

http://www.eyesondarfur.org

http://www.rand.org/methods/egoweb.html

University of Kentucky OpenEddi- http://www.uky.edu/publichealth/about/faculty-and-staff-directory/kate-eddens

http://www.valorportamaulipas.info

http://www.ushahidi.com

http://petajakarta.org/banjir/en/