GRAHAM TURNBULL ESSAY COMPETITION 2018

Wordcount: 1,961 (excluding essay title)

Is technology an opportunity or threat for human rights lawyers? Does it increase or reduce risks for lawyers in carrying out their duties and in what circumstances might technology be used to mitigate such risks?

The relevance of technology to the endeavours of human rights lawyers (HRLs) specifically relates to its ability to harness data, which presents concrete and numerous opportunities for lawyers in case-building, fact-finding and evidence-gathering efforts. These advantages must however be weighed against the real threat to the right of privacy of individuals whose data is collected, accessed or used for human rights enforcement purposes. The role of HRLs has accordingly and necessarily evolved to include a balancing exercise between rights – those that they seek to enforce through litigation relying upon technology, and those that are threatened by this very undertaking. This essay argues that, whilst the use of technology in HRL's work entails a risk to privacy rights that cannot be fully eradicated, this risk is sufficiently mitigated to warrant the continued reliance on technology for accountability efforts. For the purposes of this competition, technology will be understood to encompass the tools, platforms and processes involved in collecting, accessing and using data. In assessing its relevance to human rights lawyers, this paper will consider their functions both as researchers and litigators.

An underutilised path to accountability for human rights violations

The combination of multiple tech breakthroughs and the dissemination of low-cost technological equipment among traditionally non-privileged groups have created a unique landscape – and opportunity – for the promotion and enforcement of human rights. Technology can be an asset in improving a specific case's chances of success, and widening the range of actionable human rights claims. Among the countless tech innovations in the field, three developments are increasingly relied upon by HRLs as evidence in international accountability, fact-finding and litigation efforts.

Geospatial technology is the most established in terms of reliability and use as evidence by legal practitioners and courts alike. For example, digital satellite imagery has played a significant role

in proceedings before regional human rights courts protecting the rights of indigenous communities and asylum-seekers through land-mapping[1] and tracking of migration trends.[2] Forensic architecture technology – which also relies on satellite communications – is its most impressive iteration, enabling the recreation of buildings and urban environments in the form of architectural evidence through 3D modelling and interactive audiovisual representations.[3] Although such evidence is yet to be accepted by courts, there is promise in that other human rights agencies – including the UN – have relied on these efforts.[4]

The proliferation of platforms enabling first-hand video recordings documenting human rights abuses is another significant tech development, not least because they provide valuable information to establish facts relating to the unlawful act, perpetrator(s), and victim(s) which HRLs can present before domestic or international courts. Some are equipped with features ensuring the evidentiary value of the video, including inbuilt verification processes through metadata capture and secure storage through a trackable chain of custody.[5]

Yet the most ground-breaking development is the increasing use of open source intelligence (OSINT), an investigative method using publicly available data in all its forms to establish facts. Whilst the use of open source information is yet to become established in legal proceedings against grave human rights violations, there have been a few significant steps in this direction in which the International Criminal Court (ICC) has been a crucial actor. The ICC Prosecutor produced numerous open source materials in the list of evidence in the trial against Ahmad Al-Mahdi.[6] These open source materials reportedly attested to the destruction of relevant archaeological sites of religious and historic character through video footage and satellite

[1] Inter-American Court of Human Rights (IACtHR), *Sawhoyamaxa Indigenous Community v Paraguay* (2006)
[2] European Court of Human Rights (ECtHR), *Sufi and Elmi v United Kingdom* (2011).
[3] Forensic Architecture, 'Project' < https://www.forensic-architecture.org/project/> accessed 13 November 2018.
[4] UN OHCHR, Statement by Ben Emerson, UN Special Rapporteur on Terrorism and Human Rights, 24 January 2012.
[5] EyeWitness Project, 'Using the App' <https://www.eyewitnessproject.org/#> accessed 13 November 2018.
[6] Statement of the Prosecutor of the ICC, Fatou Bensouda, in the opening of Trial in the against Mr Ahmad Al-Faqi Al-Mahdi.

imagery.[7] Similarly, the first arrest warrant issued in the Al-Werfalli case significantly relied on videos posted on social media as an information source.[8]

Whilst the ultimate reliability of these materials is subject to each courts' rules of evidence and discretion, HRLs play a significant and unique role in making the case for their admissibility as evidence. But technology – taken on its own – can only go so far in legal proceedings without a witness or expert witness corroborating the data involved. A recent cross-jurisdictional study suggests that what makes material sourced through modern technology persuasive is not the technology itself, but the credibility of the person validating its content.[9] Even so, the availability of technology can bolster the strength of a human rights case by providing direct or circumstantial evidence in support of a victim's allegations.

A wieldy sword of Damocles

The well-documented risks customarily involved in the use of technology acquire an additional layer of complexity – and liability – when considered in light of lawyers' professional duties relating to integrity, confidentiality and their obligation to act in their client's best interests. Each of these challenges and their corresponding solutions will be addressed in turn. Where the personal data of individuals is at issue, the legal framework applied to the analysis will be the General Data Protection Regulation (GDPR). To the extent that HRLs' carry out operations on a third party's personal data – known as "data processing" under Article 4(2) GDPR – for the purposes of providing legal services in connection with their clients' instructions, they are data controllers within the meaning of GDPR. [10]

First, technology can be weaponised to access and use confidential information relating to the client and her case. Under Article 24 GDPR, HRLs undertake an obligation to implement appropriate technical and organizational measures to ensure that data processing is carried out in accordance with GDPR, taking into account the nature, scope, contexts and purposes of processing as well as the varying likelihood and severity for the rights and freedoms of natural

[7] ICC, *The Prosecutor v. Ahmad Al Faqi Al-Mahdi*, Transcript of Trial Hearing of 22 August 2016, ICC-01/12-01/15, 100.
[8] ICC, *The Prosecutor v. Mahmoud Al-Werfalli*, Warrant of Arrest of 15 August 2017, ICC-01/11-01/17, 4,8.
[9] AAAS, *Geospatial Evidence in International Human Rights Litigation* (AAAS 2008), 31.
[10] ICO, *Data Controllers and Data Processors* (ICO 2014), para. 42; Bar Council, *GDPR: Bar Council Guide for Barristers and Chambers* (2017), para.4.

persons.[11] An information breach, whatever the circumstances, will therefore compromise the fulfilment of HRLs' professional secrecy obligation and their duty to act in the best interests of their client. An information leak may render a legal strategy ineffective by revealing key legal arguments and enabling the manipulation of leaked information, thus jeopardising the credibility of the victim(s) and witnesses.[12] In addition to disciplinary action, a failure to apply appropriate safeguarding measures will result in liability under the GDPR. In a 2017 decision, the Information Commissioner's Office (ICO) fined a barrister under the Data Protection Act – GDPR's predecessor – after confidential case files stored in a family computer were leaked online, finding that the barrister had breached a provision equivalent to GDPR's Article 24. The ICO acknowledged in that case that encryption of the files would have sufficed to protect the barrister from liability.[13]

But the dire consequences of a data breach may extend far beyond the scope of the legal case or indeed GDPR compliance. There is consensus among human rights agencies that the revealed identities of activists, victims, witnesses and survivors may translate into a security threat leading to their torture and ill-treatment in retaliation.[14] These risks can however be considerably mitigated through pseudonymisation and encryption of data, a digital process ensuring that only the intended recipient is able to read the communications transmitted to them.[15] The value of encryption as a critical tool for HRLs has been reiterated by human rights and tech organisations alike, which have described it as an essential means of protection of individuals' rights to privacy and free speech. [16] Given the nature of human rights proceedings, any leak is likely to involve a special category of personal data – that is data related to an individual's ethnic origin, political opinions, religious or philosophical beliefs, sex life or sexual orientation – and thus requires a greater standard of care.[17] It is therefore fundamental for HRLs to use both device and end-to-end encryption to ensure they effectively minimise risk.[18] Through password-protection of devices and the use of social media platforms where the content of communications between users are

[11] GDPR, Art.24(1).
[12] OHCHR, *Training Manual on Human Rights Monitoring: The Monitoring Function* (2001), para.11.
[13] ICO, Decision of 16 March 2017, para. 45.
[14] WITNESS, *Cameras Everywhere* (WITNESS 2011), 19; UNHRC, *Summary of the Human Rights Council panel discussion on the right to privacy in the digital age*, 19 December 2014, A/HRC/28/39, para.6; Sanja Kelly et al., *Silencing the Messenger: Communication Apps under Pressure* (Freedom House 2016), 1-3.
[15] GDPR, Art. 32(1).
[16] Amnesty International, *Encryption: A Matter for Human Rights* (Amnesty 2016), 3-4; Amnesty International, Benetech, and the Engine Room, *DatNav*, 68.
[17] GDPR, Art. 9.
[18] Amnesty International, *Encryption: A Matter for Human Rights* (Amnesty 2016), 21-24.

impossible to decrypt by anyone other than themselves, respectively, encryption significantly mitigates the risk of leaks.

In a similar vein, a lawyer's integrity may be called into question if evidence is presented at the expense of other individuals' privacy rights – including the alleged perpetrator of a human rights violation, or other individuals depicted in the materials relied upon in the proceedings. HRLs must ensure that only such third party personal data as is relevant to the case is processed, and only to an extent proportionate to the need. The processing of a third party's data by HRLs will not be an issue under GDPR if necessary in order to protect the client's vital interests or legitimate interests,[19] of which human rights enforcement may be an example.

Lastly, HRL's careless use of technology may threaten their perceived honesty and integrity. Even with the best of intentions, a HRL's failure to detect (i) staged content, (ii) doctored content or (ii) doctored metadata – the most prevalent form of deception as reported by HRLs –[20] in the materials they seek to submit as evidence may legitimately rouse suspicion as to whether this was a deliberate attempt to mislead the court. It is however possible to minimise any possible instances of manipulation of evidence by securing a chain of custody of the materials relevant to the case.[21] Similarly, if the information was acquired through OSINT, the use of verification methods may reassure HRLs of the degree of reliability of the materials they seek to submit. Multiple verification tools exist at HRLs' fingertips, ranging from platforms automatically revealing the metadata of photos and videos to websites which act as repositories of defunct web pages.[22]

Conclusion

Technology can play a significant role in both enforcing and undermining human rights. In light of the general obligation for lawyers to act in the best interests of their clients,[23] it is the responsibility of HRLs to harness the power of technology to ensure no opportunity is missed to ensure accountability for human rights violations. However, tech-based solutions are only one avenue at the disposal of HRLs to maximise their effective use of technology. And there is such a reckoning

[19] GDPR, Art.6(1)(d), (f).
[20] C Koettl, *Citizen Media Research and Verification: An Analytical Framework for Human Rights Practitioners* (CUP 2016), 16.
[21] Amnesty International, Benetech, and the Engine Room, *DatNav*, 36.
[22] European Journalism Centre, *The Verification Handbook* (EJC 2014), 108-110.
[23] IBA, *International Principles on Conduct for the Legal Profession* (IBA 2011), Principle 5.1.

among HRLs: in 2017, a group of practitioners, investigators and journalists drafted the first ever set of ethical principles applicable to the instrumentalisation of open source information for case-building and litigation. [24] It is therefore hoped that this trend will consolidate in future.

[24] UC Berkeley Human Rights Center, *The New Forensics* [The Bellagio Report] (2018).